COOPER BLAZER INC.

ANTI-MONEY LAUNDERING (AML)/ ECONOMIC AND FINANCIAL SANCTIONS COMPLIANCE POLICY

Approved Date: 03.08.2025

TABLE OF CONTENTS

ANTI-MONEY LAUNDERING PROGRAM 2

1. Records Retention 4
2. Designation of AML Compliance Officer 5
3. Section 314 Information Sharing. 5
4. Checking the Office of Foreign Assets Control Listings 8
5. Customer Identification Program 8
6. Customer Due Diligence Rule 13
7. Correspondent Accounts for Foreign Shell Banks 14
8. Due Diligence and Enhanced Due Diligence Requirements 15
9. Senior Foreign Politically Figures 17
10. Section 311 Special Measures 18
11. Monitoring Accounts for Suspicious Activity 18
12. Suspicious Transactions and BSA Reporting 21
13. Independent Review of AML Program 24
14. AML Recordkeeping 24
15. Clearing/Introducing Company Relationships 25
17. Monitoring Employee Conduct and Accounts 26
18. Confidential Reporting of AML Non-Compliance (Whistle-blower protection)) 26
19. Additional Risk Areas 26
20. Senior Manager Approval 26

Attachment A – Restricted Activities List 27

Attachment B – Money Laundering Risk Assessment 27

Attachment C – Risk Scorecard and EDD Risk Scorecard 36

Appendix A: CDD Score Card 37

ANTI-MONEY LAUNDERING PROGRAM

Cooper Blazer Inc. (referred to as the "Company") has a strict policy to prohibit and actively prevent money laundering, as well as any activity that aids money laundering or the financing of terrorist or criminal activities. This commitment is upheld by complying with all relevant obligations under the Bank Secrecy Act (BSA) and its corresponding regulations.

Money laundering is generally defined as actions 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 traveller’s checks, or deposited into accounts at financial institutions. At the “layering” stage, funds are transferred or moved into other accounts or other financial institutions to 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 of 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.

These anti-money laundering (“AML”) policies, procedures, and internal controls are designed to ensure compliance with all applicable BSA regulations and will be reviewed and updated on a regular basis to ensure Cooper Blazer maintains appropriate policies, procedures, and internal controls to account for both changes in regulations and changes in our business.

The Cooper Blazer AML Program is built upon the following four fundamental principles:

Internal Controls

Cooper Blazer shall provide for a system of internal controls, policies, and procedures designed to ensure ongoing compliance with all applicable AML laws, rules, and regulations.

Independent Testing

Cooper Blazer shall provide for independent testing for compliance with, and the effectiveness of, the AML program to be conducted by qualified internal personnel of Cooper Blazer, who is not responsible for the design, installation, maintenance, or operation of the AML program, or the policies and procedures that guide its operation, or a qualified external party, at least annually, the findings of which shall be summarized in a written report submitted to the Chief Executive Officer of Cooper Blazer, the Board of Directors of Cooper Blazer, and, if required, applicable regulatory authorities.

Designation of an AML Officer

Cooper Blazer shall appoint a qualified individual or individuals to oversee and manage day-to-day compliance with its Anti-Money Laundering (AML) program.

Catherine Ramos has been designated as the AML Officer for Cooper Blazer. In this role, Ms. Ramos is responsible for coordinating and monitoring daily compliance with the Cooper Blazer AML Program. She will also initiate training modules related to AML proficiency for applicable employees and may designate any member of the Cooper Blazer staff to assist her in fulfilling this responsibility.

The AML Officer's responsibilities include all of the following:

- Monitoring changes in AML laws, including updated OFAC and SDN lists (defined below), and updating the program accordingly;
- Maintaining all books and records required to be created and retained under this policy;
- Reviewing all filings required under this policy before submission;
- Escalating matters to the board of directors, senior management, or appropriate governing body and seeking outside counsel, as appropriate;
- Providing periodic reporting, at least annually, to the board of directors, senior management, and other appropriate governing body, as applicable; and
- Ensuring compliance with relevant training requirements.

Ongoing Training

Cooper Blazer shall provide ongoing training for appropriate personnel to:

1. Ensure they understand Cooper Blazer's AML requirements
2. Enable them to identify transactions required to be reported to applicable regulatory authorities.
3. Maintain records required to be kept in accordance with Cooper Blazer's AML program.

Cooper Blazer will consider a variety of service providers, products, and events from the United States Department of the Treasury Financial Crimes Enforcement Network ("FinCEN"), the Practicing Law Institute, and ACAMS, among other organizations dedicated to enhancing knowledge, skill, and expertise of AML requirements, to provide AML training to appropriate Cooper Blazer personnel.

1. Records Retention

The company shall maintain the records listed below for a period of five years and keep them readily available for inspection as required by law. Additionally, the company has developed an internal mechanism to detect the following:

- Details pertaining to user transaction, including but not limited to
    - The nature of the transaction;
    - the amount of the transaction and the currency in which it was denominated;
    - the date on which the transaction was conducted; and
    - the parties to the transaction

- All details for the following categories of user transaction, separately from those recorded above:
    - User transactions of value of at least $10,000 or its foreign currency equivalent; and
    - User transactions that are connected to each other and that take place within a month of each other, with a monthly aggregate of at least $ 100,000 or its foreign currency equivalent; and

- All Suspicious Transactions by way of deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of:
    - checks including third party cheques, pay orders, demand drafts, or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits; or
    - transfers from one account within the same banking company, financial institution, and intermediary, including to and from Nostro and Vostro accounts; or
    - any other mode in whatsoever name it is referred to;

- Money transfer or remittances in favor of own Users or non-Users from the US or abroad and to third party beneficiaries in the US or abroad, including transactions on its own account in any currency by any of the following:
    - Money Orders
    - Wire Transfer or Electronic transfers
    - Internal Transfer
    - Automated Clearing House remittance
    - Any other mode of money transfer by whatsoever name is called.

- Procedure and Manner for Marinating Information
    - Cooper Blazer will maintain hard and soft copies of the above-mentioned records of Transactions in accordance with the procedure and manner, as may be specified under applicable laws or regulations, from time to time;
    - In addition to the above, Cipher shall maintain records of transactions as per its prevailing processes.

2. Designation of AML Compliance Officer

The Company has designated Catherine Ramos as its Anti-Money Laundering Program Compliance Officer ("AML Compliance Officer"), with full responsibility for the Company's AML program. AML Compliance Officer has a working knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge, and training. The AML Compliance Officer is vested with full responsibility and authority to enforce the Company's AML program.

The duties of the AML Compliance Officer will include the following:

- Assisting with the development, implementation, and maintenance of an anti-money laundering program within their institution.
- Ensuring compliance with current AML regulations, and other relevant legislation
- Developing and maintaining a risk assessment framework for products and services, clients and customers, and other issues relating to money laundering.
- Keeping and maintaining records of high-risk customers and reporting suspicious activities to the authorities.
- Arranging and implementing inspections and audits from third-party organizations and making compliance recommendations based on their findings.
- Briefing and reporting to senior management on matters relating to internal AML compliance policies and procedures.
- Overseeing and implementing an ongoing AML training program for other employees.

3. Section 314 Information Sharing.

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

We will respond to a Financial Crimes Enforcement Network (FinCEN) request concerning accounts and transactions (a 314(a) Request) by immediately searching our records to determine whether we maintain or have 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 website. We understand that we have 14 days (unless otherwise specified by FinCEN) from the transmission date of the request to respond to a 314(a) Request.

We 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 contact information for the AML Compliance Person.) Unless otherwise stated in the 314(a) Request or specified by FinCEN, we are required to search those documents outlined in FinCEN's FAQ. If we find a match, the Company's "AML Contact Person in FCS" 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 Company will structure our search accordingly. If the search of our records does not show a matching account or transaction, then Company will not reply to the 314(a) Request.

We will not disclose that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. The Company will review, maintain and implement procedures to protect the security and confidentiality of requests from FinCEN similar to those procedures established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act with regard to the protection of customers' nonpublic information.

We will direct any questions 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, we will not be required to treat the information request as continuing in nature, and we 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

We understand that receiving a National Security Letter (NSL) is highly confidential. We understand that none of our officers, employees, or agents may directly or indirectly disclose to any person the FBI or other federal government authority has sought or obtained access to any of our records. To maintain the confidentiality of any NSL we receive, we will process and maintain the NSL by dating and time stamping all such items on receipt, maintaining a log of all services received, and copies of all documentation related to the investigation. If we file a SAR after receiving an NSL, the SAR will not contain any reference to the receipt or existence of the NSL. The SAR will only contain detailed information about the facts and circumstances of the detected suspicious activity.

c. Grand Jury Subpoenas

We understand that the receipt of a grand jury subpoena concerning a customer does not require that we file a Suspicious Activity Report (SAR). When we receive a grand jury subpoena, we will conduct a risk assessment of the customer subject to the subpoena and review the customer's account activity. If we uncover suspicious activity during our risk assessment and review, we will elevate that customer's risk assessment and file a SAR in accordance with the SAR filing requirements.

We understand that none of our 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 we used to respond to it. To maintain the confidentiality of any grand jury subpoena we receive, we will process and maintain the subpoena through our Registered Agent. If we file a SAR after receiving a grand jury subpoena, the SAR will not contain any reference to the receipt or existence of the subpoena. The SAR 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)

We will share information with other financial institutions regarding individuals, entities, organizations, and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering. We will ensure that the Company files with FinCEN an initial notice before any sharing occurs and annual notices thereafter. We will use the notice form found on FinCEN's website. Before we share information with another financial institution, we 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 FinCEN will make available. We understand that this requirement applies even to financial institutions with which we are affiliated and that we will obtain the requisite notices from affiliates and follow all required procedures.

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

We 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.

e. Joint Filing of suspicious activity report (SARs) by Broker-Dealers and Other Financial Institutions

We will file joint SARs in the following circumstances, according to Section 356 of the USA PATRIOT Act amended as BSA, a Broker-Dealer is required to file suspicions activity report (i) a transaction is conducted or attempted to be conducted by, at, or through a broker-dealer; (ii) the transaction involves or aggregates funds or other assets of at least $5,000; and (iii) the broker-dealer knows, suspects, or has reason to suspect that the transaction funds are derived from illegal activity. We will also share

information about a particular suspicious transaction with any broker-dealer, as appropriate, involved in that particular transaction for purposes of determining whether we will file a SAR jointly.

We will share information about particular suspicious transactions with our clearing broker to determine whether our clearing broker and we will file a SAR jointly. In cases where we file a joint SAR for a transaction handled both by the clearing broker and us, we may share a copy of the filed SAR with the clearing broker.

If we determine it is appropriate to jointly file a SAR, we understand that we cannot disclose that we have filed a SAR to any financial institution except the financial institution that is filing jointly. If we determine it is not appropriate to file jointly, we understand that we cannot disclose that we have filed a SAR to any other financial institution or insurance company.

4. Checking the Office of Foreign Assets Control Listings

Before opening an account, and on an ongoing basis, the Company will check to ensure that a customer does not appear on the SDN list or is not engaging in transactions prohibited by the economic sanctions and embargoes administered and enforced OFAC. (See the OFAC website 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, we will consult them regularly and subscribe to receive any available updates as soon as they occur. With respect to the SDN list, Company may also access that list through various software programs to ensure speed and accuracy. See also FINRA's OFAC Search Tool that screens names against the SDN list. We will also review existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated. AML Compliance Officer will document the review.

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

Our review will include but is not limited to customer accounts, transactions involving customers (including activity that passes through the Company's platform such as wires), and the review of customer transactions that involve physical cryptocurrencies.

5. Customer Identification Program

Cooper Blazer shall maintain a Customer Identification Program ("CIP"). The CIP shall include the following measures and efforts: We will collect certain minimum customer identification information from each customer who opens an account; utilize risk-based measures to verify the identity of each customer who opens an account; record customer identification information and the verification methods and results; provide the required adequate notice to customers that Company will seek identification information to verify their

identities if applicable; and compare customer identification information with government-provided lists of suspected terrorists, once the government has issued such lists. See Section 5.g. (Notice to Customers) for additional information.

We will also collect information to determine whether any entity opening an account would be excluded as a "customer," pursuant to the exceptions outlined in 31 CFR 1023.100(d)(2)) (e.g., documentation of a company's listing information, licensing or registration of a financial institution in the US, and status or verification of the authenticity of a government agency or department).

a. Required Customer Information

Prior to opening an account, our AML Compliance Officer will collect the following information for all accounts, if applicable, for any person, entity, or organization that is opening a new account and whose name is on the account:

(1) the name;

(2) date of birth (for an individual);

(3) 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

(4) an identification number, which will be a taxpayer identification number (for US 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).

When opening an account for a foreign business or enterprise that does not have an identification number, we will request alternative government-issued documentation certifying the existence of the business or enterprise.

b. Customers Who Refuse to Provide information

If a potential or existing customer either refuses to provide the information described above when requested or appears to have intentionally provided misleading information, Company will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, our AML Compliance Officer will be notified so that we can determine whether we should report the situation to appropriate governing bodies.

c. Verifying Information

Based on the risk, and to the extent reasonable and practicable, we will ensure that the company has a reasonable belief that it knows the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. Our AML Compliance Officer will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the customer's true identity is real.

We will verify customer identity through documentary means, non-documentary means, or both. We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement documentary evidence by using the non-documentary means described below whenever necessary. We may also use non-documentary means if the Company is still uncertain about whether we know the customer's true identity. In verifying the information, we will consider whether the identifying information that The Company receives, such as the customer's name, street address, zip code, telephone number (if provided), date of birth, and Social Security number, allows us to determine that Company has a reasonable belief that we know the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).

Appropriate documents for verifying the identity of customers include the following:

- For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguards, such as a driver's license or passport; and

- For a person other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument.

- Company understands that it's not required to take steps to determine whether the document that the customer has provided for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. However, we note that the document shows some obvious form of fraud. We must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity.

We will use the following non-documentary methods of verifying identity:

- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other sources

- Checking references with other financial institutions; or

- Obtaining a financial statement.

- Utilize third-party identity verification services

We will use non-documentary methods of verification when:

(1) the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;

(2) Company is unfamiliar with the documents the customer presents for identification verification;

(3) the customer and Company do not have face-to-face contact; and

(4) there are other circumstances that increase the risk that we will be unable to verify the customer's true identity through documentary means.

We will verify the information within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information. In some instances, when we need more time, we may, pending verification, restrict the types of transactions or dollar amount transactions. If we find suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, we will, after internal consultation with our AML Compliance Officer, file a SAR in accordance with applicable laws and regulations.

The Company recognizes that the risk that it may not know the customer's true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership, or trust that is created or conducts substantial business in a jurisdiction that we have designated as a primary money laundering jurisdiction, a terrorist concern, or has been designated as a non-cooperative country or territory. We will identify customers that pose a heightened risk of not being properly identified.

d. Lack of Verification

When Company cannot form a reasonable belief that it knows the true identity of a customer, Company will do the following: (1) not open an account; (2) impose terms under which a customer may conduct transactions while Company attempts to verify the customer's identity; (3) close an account after attempts to verify a customer's identity fail; and (4) determine whether it is necessary to report to appropriate agencies in accordance with applicable laws and regulations.

e. Recordkeeping

We will document its verification, including all identifying information provided by a customer, the methods used and verification results, and the resolution of any discrepancies identified in the verification process. We will keep records containing a description of any document that is relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify a customer's identity. We will also keep records containing a description of the resolution of each substantive discrepancy

discovered when verifying the identifying information obtained. We will retain records of all identification information for five years after the account has been closed; we will retain records made about verification of the customer's identity for five years after the record is made.

f. Comparison with Government-Provided Lists of Terrorists

At such time as Company receives notice that a federal government agency has issued a list of known or suspected terrorists and identified the list as a list for CIP purposes, we will, within a reasonable period of time after an account is opened (or earlier, if required by another federal law or regulation or Federal directive issued in connection with an applicable list), determine whether a customer appears on any such list of known or suspected terrorists or terrorist organizations issued by any federal government agency and designated as such by Treasury in consultation with the federal functional regulators. We will follow all federal directives issued in connection with such lists.

We will continue to comply separately with OFAC rules prohibiting transactions with certain foreign countries or their nationals.

g. Notice to Customers

We will notify customers that the company is requesting information from them to verify their identities, as required by federal law.

To help the government fight the funding of terrorism and money laundering activities, federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account.

When customers open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

h. Reliance on Another Financial Institution for Identity Verification

We may, under the following circumstances, rely on the performance by another financial institution (including an affiliate) of some or all of the elements of our CIP with respect to any customer that is opening an account or has established an account or similar business relationship with the other financial institution to provide or engage in services, dealings, or other financial transactions:

- when such reliance is reasonable under the circumstances;

- when the other financial institution is subject to a rule implementing the anti-money laundering compliance program requirements of 31 USC § 5318(h) and is regulated by a federal functional regulator; and

- when the other financial institution has entered into a contract with Company requiring it to certify annually to us that it has implemented its anti-money laundering program and that it will perform (or its agent will perform) specified requirements of the customer identification program.

6. Customer Due Diligence Rule

In addition to the information collected under the Customer Identification Program, we have established, documented, and maintained written policies and procedures reasonably designed to identify and verify beneficial owners of legal entity customers and comply with other aspects of the Customer Due Diligence (CDD) Rule. We will collect minimum CDD information from beneficial owners of legal entity customers. We will understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile. We will conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, maintain and update customer information.

a. Identification and Verification of Beneficial Owners

At the time of opening an account for a legal entity customer, Company will identify any individual that is a beneficial owner of the legal entity customer by identifying any individuals who directly or indirectly own 25% or more of the equity interests of the legal entity customer, and any individual with significant responsibility to control, manage, or direct a legal entity customer. The following information will be collected for each beneficial owner:

(1) the name;

(2) date of birth (for an individual);

(3) an address, which will be a residential or business street address (for an individual), or 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); and

(4) an identification number, which will be a Social Security number (for US persons), or one or more of the following: a passport number and country of issuance, or other similar identification numbers, such as an 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).

For verification, we will describe any document relied on (noting the type, any identification number, place of issuance, and, if any, date of issuance and expiration). We will also describe any non-documentary methods and the results of any measures undertaken.

b. Understanding the Nature and Purpose of Customer Relationships

We will understand the nature and purpose of customer relationships to develop a customer risk profile through the following methods:

- The type of customer;
- The account or service being offered;
- The customer's domicile;
- The customer's principal occupation or business; and
- In the case of existing customers, the customer's history of activity.

c. Conducting Ongoing Monitoring to Identify and Report Suspicious Transactions

We will conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, maintain and update customer information, including information regarding the beneficial ownership of legal entity customers, using the customer risk profile as a baseline against which customer activity is assessed for suspicious transaction reporting. Our suspicious activity monitoring procedures are detailed within Section 11 (Monitoring Accounts for Suspicious Activity).

7. Correspondent Accounts for Foreign Shell Banks

a. Detecting and Closing Correspondent Accounts of Foreign Shell Banks

We will identify foreign bank accounts and any such account that is a correspondent account (any account that is established for a foreign bank to receive deposits from, or to make payments or other disbursements on behalf of, the foreign bank, or to handle other financial transactions related to such foreign bank) for foreign shell banks. Upon finding or suspecting such accounts, Company employees will notify the AML Compliance Person, who will terminate any verified correspondent account in the United States for a foreign shell bank. We will also terminate any correspondent account that we have determined is not maintained by a foreign shell bank but is being used to provide services to such a shell bank. We will exercise caution regarding liquidating positions in such accounts and take reasonable steps to ensure that no new positions are established in these accounts during the termination period. We will terminate any correspondent account for which we have not obtained the information described in the regulations regarding shell banks within the time periods specified in those regulations.

b. Certifications

We will require our foreign bank account holders to identify the owners of the foreign bank if it is not publicly traded, the name and street address of a person who resides in the United States and is authorized and has agreed to act as agent for acceptance of legal process, and an assurance that the foreign bank is not a shell

bank nor is it facilitating the activity of a shell bank. In lieu of this information, the foreign bank may submit the Certification Regarding Correspondent Accounts for Foreign Banks provided in the BSA regulations. We will re-certify when we believe that the information is no longer accurate or at least once every three years.

c. Recordkeeping for Correspondent Accounts for Foreign Banks

We will keep records identifying the owners of foreign banks with US correspondent accounts and the name and address of the US agent for service of legal process for those banks.

d. Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationships with Foreign Bank

When we receive a written request from a federal law enforcement officer for information identifying the non-publicly traded owners of any foreign bank for which we maintain a correspondent account in the United States and/or the name and address of a person residing in the United States who is an agent to accept service of legal process for a foreign bank's correspondent account, we will provide that information to the requesting officer not later than seven days after receipt of the request. We will close, within 10 days, any correspondent account for a foreign bank that we learn from FinCEN or the Department of Justice has failed to comply with a summons or subpoena issued by the Secretary of the Treasury or the Attorney General of the United States or has failed to contest such a summons or subpoena. We will scrutinize any correspondent account activity during that 10-day period to ensure that any suspicious activity is appropriately reported and to ensure that no new positions are established in these correspondent accounts.

8. Due Diligence and Enhanced Due Diligence Requirements

a. Due Diligence for Correspondent Accounts of Foreign Financial Institutions

We will conduct an inquiry to determine whether a foreign financial institution has a correspondent account established, maintained, administered, or managed by the Company.

If we have correspondent accounts for foreign financial institutions, we will assess the money laundering risk posed based on a consideration of relevant risk factors. We can apply all or a subset of these risk factors depending on the nature of the foreign financial institutions and the relative money laundering risk posed by such institutions.

The relevant risk factors can include:

- the nature of the foreign financial institution's business and the markets it serves;
- the type, purpose, and anticipated activity of such correspondent account;
- the nature and duration of the Company's relationship with the foreign financial institution and its affiliates;

- the anti-money laundering and supervisory regime of the jurisdiction that issued the foreign financial institution's charter or license and, to the extent reasonably available, the jurisdiction in which any company that is an owner of the foreign financial institution is incorporated or chartered; and

- information known or reasonably available to the covered financial institution about the foreign financial institution's anti-money laundering record.

In addition, our due diligence program will consider additional factors that have not been enumerated above when assessing foreign financial institutions that pose a higher risk of money laundering.

We will apply our risk-based due diligence procedures and controls to each foreign financial institution's correspondent account on an ongoing basis. This includes periodically reviewing the activity of each foreign financial institution correspondent sufficient to ensure whether the nature and volume of account activity are generally consistent with the information regarding the purpose and expected account activity and to ensure that the Company can adequately identify suspicious transactions. Ordinarily, we will not conduct this periodic review by scrutinizing every transaction taking place within the account. One procedure we may use instead is to use any account profiles for our correspondent accounts (to the extent we maintain these) that we ordinarily use to anticipate how the account might be used and the expected volume of activity to help establish baselines for detecting unusual activity

b. Enhanced Due Diligence

We will assess any correspondent accounts for foreign financial institutions to determine whether they are correspondent accounts that have been established, maintained, administered, or managed for any foreign bank that operates under:

(1) an offshore banking license;

(2) a banking license issued by a foreign country that has been designated as non-cooperative with international anti-money laundering principles or procedures by an intergovernmental group or organization of which the United States is a member and with which designation the US representative to the group or organization concurs; or

(3) a banking license issued by a foreign country that has been designated by the Secretary of the Treasury as warranting special measures due to money laundering concerns.

If we determine that we have any correspondent accounts for these specified foreign banks, we will perform enhanced due diligence on these correspondent accounts. The enhanced due diligence that we will perform for each correspondent account will include, at a minimum, procedures to take reasonable steps to:

(1) conduct enhanced scrutiny of the correspondent account to guard against money laundering and identify and report any suspicious transactions. Such scrutiny will not only reflect the risk assessment that is described in Section 8.a. above, but will also include procedures to, as appropriate:

(i) obtain (e.g., using a questionnaire) and consider information related to the foreign bank's AML program to assess the extent to which the foreign bank's correspondent account may expose us to any risk of money laundering;

(ii) monitor transactions to, from or through the correspondent account in a manner reasonably designed to detect money laundering and suspicious activity (this monitoring may be conducted manually or electronically and may be done on an individual account basis or by-product activity); and

(iii) obtain information from the foreign bank about the identity of any person with authority to direct transactions through any correspondent account that is payable-through (a correspondent account maintained for a foreign bank through which the foreign bank permits its customer to engage, either directly or through a subaccount, in banking activities) and the sources and beneficial owners of funds or other assets in the payable-through account.

(2) determine whether the foreign bank maintains correspondent accounts for other foreign banks that enable those other foreign banks to gain access to the correspondent account under review and, if so, to take reasonable steps to obtain information to assess and mitigate the money laundering risks associated with such accounts, including, as appropriate, the identity of those other foreign banks; and

(3) if the foreign bank's shares are not publicly traded, determine each owner's identity and the nature and extent of each owner's ownership interest. We understand that for purposes of determining a private foreign bank's ownership, an "owner" is any person who directly or indirectly owns, controls or has the power to vote 10 percent or more of any class of securities of a foreign bank. We also understand that members of the same family shall be considered to be one person.

c. Special Procedures When Due Diligence or Enhanced Due Diligence Cannot Be Performed

In the event there are circumstances in which we cannot perform appropriate due diligence with respect to a correspondent account, we will determine, at a minimum, whether to refuse to open the account, suspend transaction activity, file a SAR, close the correspondent account and/or take other appropriate action.

9. Senior Foreign Politically Figures

We will review our accounts to determine whether we offer any private banking accounts, and we will conduct due diligence on such accounts. This due diligence will include at least: (1) ascertaining the identity of all nominal holders and holders of any beneficial ownership interest in the account (including information on those holders' lines of business and sources of wealth); (2) ascertaining the source of funds deposited into the account; (3) ascertaining whether any such holder may be a senior foreign political figure; and (4) detecting

and reporting, in accordance with applicable laws and regulations, any known or suspected money laundering, or use of the proceeds of foreign corruption.

We will review public information, including information available in Internet databases, to determine whether any private banking account holders are senior foreign political figures. If we discover information indicating that a particular private banking account holder may be a senior foreign political figure, and upon taking additional reasonable steps to confirm this information, we determine that the individual is, in fact, a senior foreign political figure, we will conduct additional enhanced due diligence to detect and report transactions that may involve money laundering or the proceeds of foreign corruption.

In so doing, we will consider the risks that the funds in the account may be the proceeds of foreign corruption by determining the purpose and use of the private banking account, location of the account holder(s), source of funds in the account, type of transactions conducted through the account and jurisdictions involved in such transactions. The degree of scrutiny we will apply will depend on various risk factors, including, but not limited to, whether the jurisdiction the senior foreign political figure is from is one in which current or former political figures have been implicated in corruption and the length of time that a former political figure was in office. Our enhanced due diligence might include, depending on the risk factors, probing the account holder's employment history, scrutinizing the account holder's source(s) of funds, and monitoring transactions to the extent necessary to detect and report proceeds of foreign corruption and reviewing monies coming from the government, government-controlled or government enterprise accounts (beyond salary amounts).

If we do not find information indicating that a private banking account holder is a senior foreign political figure, and the account holder states that he or she is not a senior foreign political figure, then we may make an assessment if a higher risk for money laundering, nevertheless, exists independent of the classification. If a higher risk is apparent, we will consider additional due diligence measures to ensure all the requirements are met.

In either case, if due diligence (or the required enhanced due diligence, if the account holder is a senior foreign political figure) cannot be performed adequately, we will, after consultation with the Company's AML Compliance Person and, as appropriate, not open the account, suspend the transaction activity, file a SAR, close the account and/or take other appropriate action.

10. Section 311 Special Measures

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, Company understands that it must read FinCEN's final rule and follow any prescriptions or prohibitions contained in that rule.

11. Monitoring Accounts for Suspicious Activity

We will monitor account activity for unusual size, volume, pattern, or type of transactions, taking into account risk factors and red flags that are appropriate to our business. (Red flags are identified in Section 11.b. below.) The customer risk profile will serve as a baseline for assessing potentially suspicious activity. Our AML Compliance Officer or his or her designee will be responsible for this monitoring, they will review any activity that our monitoring system detects and will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

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, We will immediately call an appropriate law enforcement authority. If a customer or company appears on OFAC's SDN list, we will call the OFAC Hotline at (800) 540-6322. Other contact numbers we will use are: FinCEN's Financial Institutions Hotline ((866) 556-3974) (especially to report transactions relating to terrorist activity), local US Attorney's office ((212) 637-2200), local FBI office ((212) 384-1000) and local SEC office ((21) 336-1100) (to voluntarily report such violations to the SEC in addition to contacting the appropriate law enforcement authority).

b. Red Flags

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

Customers – 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.
- Customer with no discernable reason for using Company's platform.

Efforts to Avoid Reporting and Recordkeeping

- Reluctant to provide information needed to file reports or fails to proceed with transaction.
- Tries to persuade an employee not to file required reports or not to maintain required records.
- "Structures" deposits, withdrawals, or purchase of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements.

- Unusual concern with Company compliance with government reporting requirements and Company AML policies.

Certain Funds Transfer Activities

- Wire transfers to/from financial secrecy havens or high-risk geographic locations without an apparent business reason.

- Many small, incoming wire transfers or deposits are made using checks and money orders. Almost immediately withdrawn or wired out in a manner inconsistent with customer's business or history. May indicate a Ponzi scheme.

- Wire activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.

Certain Deposits or Dispositions of Cryptocurrencies

- Customer's explanation of how he or she acquired the cryptocurrency does not make sense or change.

- Customer deposits cryptocurrency with a request to transfer cryptocurrencies to multiple accounts or to sell or otherwise transfer cryptocurrencies.

Certain Cryptocurrency Transactions

- Customer has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason.

- Customer's transactions include a pattern of depositing cryptocurrencies, selling the position, and wiring out proceeds.

- Customer's trading patterns suggest that they may have inside information.

Activity Inconsistent with Business

- Transactions patterns show a sudden change inconsistent with normal activities.

- Maintains multiple accounts or maintains accounts in the names of family members or corporate entities with no apparent business or other purposes.

- Appears to be acting as an agent for an undisclosed principal but is reluctant to provide information.

Other Suspicious Customer Activity

- Unexplained high level of account activity with very low levels of securities transactions.
- Funds deposits for purchase of a long-term investment followed shortly by request to liquidate the position and transfer the proceeds out of the account.
- Law enforcement subpoenas.
- Payment by third-party check or money transfer without an apparent connection to the customer.
- Payments to third-party without apparent connection to 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 employee of Company detects any red flag or other activity that may be suspicious, he or she will notify our AML Compliance Officer immediately. Under the direction of our AML Compliance Officer, we will determine whether or not and how to investigate the matter further. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or filing a SAR.

12. Suspicious Transactions and BSA Reporting

a. Filing a SAR

We will file SARs with FinCEN for any transactions (including deposits and transfers) conducted or attempted by, at, or through our Company involving $2,000 or more of funds or assets (either individually or in the aggregate) where we know, suspect, or have reason to suspect:

(1) the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;

(2) the transaction is designed, whether through structuring or otherwise, to evade any requirements of the BSA regulations;

(3) the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and after examining the background, possible purpose of the transaction, and other facts, we know of no reasonable explanation for the transaction; or

(4) the transaction involves the use of the Company to facilitate criminal activity.

We will also file a SAR 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 we are not required to, we may contact that SEC in cases where a SAR we have filed may require immediate attention by the SEC. See Section 11 for contact numbers. We also understand that, even if we notify a regulator of a violation unless it is specifically covered by one of the exceptions in the SAR rule, we must file a SAR reporting the violation.

We may file a voluntary SAR for any suspicious transaction that we 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. Our policy is that all SARs will be reported regularly to the Board of Directors and appropriate senior management, with a clear reminder of the need to maintain the confidentiality of the SAR.

We will report suspicious transactions by completing and filing a Suspicious Activity Report (SAR) in compliance with the Bank Secrecy Act (BSA) and applicable regulatory requirements. We will collect and maintain all supporting documentation related to the suspicious activity as required by BSA regulations and our recordkeeping policies.

A SAR must be filed within **30 calendar days** from the date of initial detection of suspicious activity. If no suspect is identified at the time of initial detection, the **filing period remains 30 calendar days**. No additional extension beyond 30 days is permitted for Money Services Businesses (MSBs).

For clarity, **"initial detection"** does **not** refer to the moment when a transaction is flagged for review. Instead, it is the point at which the MSB **reasonably determines** that the activity is suspicious and meets the criteria for SAR filing under **31 CFR § 1022.320**.

An internal review must be initiated promptly upon identification of potentially suspicious activity to ensure compliance with the **non-extendable** 30-day filing deadline.

- Upon identifying **potentially suspicious activity**, an **internal review must be initiated immediately** to assess whether the transaction requires SAR filing.
- The **30-day filing period starts** when the MSB establishes that the transaction is **suspicious and reportable**, **not** when it was first flagged.

We will retain copies of any SAR filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR-SF. Upon request, we 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.

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the BSA regulations. We understand that anyone who is subpoenaed or required to disclose a SAR or the information contained in the SAR will, except where FinCEN requests disclosure, the SEC, or

another appropriate law enforcement or regulatory agency, or an SRO registered with the SEC, decline to produce the SAR or to provide any information that would disclose that a SAR was prepared or filed. We will notify FinCEN of any such request and our response.

b. Currency Transaction Reports (CTR)

Our Company prohibits transactions involving currency and has the following procedures to prevent such transactions. If we discover such transactions have occurred, we will file with FinCEN CTRs for currency transactions that exceed $10,000. Also, we will treat multiple transactions involving currency as a single transaction to determine whether to file a CTR if they total more than $10,000 and are made by or on behalf of the same person during any one business day. We will use the BSA E-Filing System to file the supported CTR Form.

c. Currency and Monetary Instrument Transportation Reports (CMIR)

Our Company prohibits both the receipt of currency or other monetary instruments that have been transported, mailed, or shipped to us from outside of the United States, and the physical transportation, mailing, or shipment of currency or other monetary instruments by any means other than through the postal service or by common carrier. We will file a CMIR with the Commissioner of Customs if we discover that we have received or caused or attempted to receive from outside of the US currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time (on one calendar day or, if for the purposes of evading reporting requirements, on one or more days). We will also file a CMIR if we discover that we have physically transported, mailed, or shipped or caused or attempted to physically transport, mail, or ship by any means other than through the postal service or by common carrier currency or other monetary instruments of more than $10,000 at one time (on one calendar day or, if for the purpose of evading the reporting requirements, on one or more days). We will use the CMIR Form provided on FinCEN's website.

d. Foreign Bank and Financial Accounts Reports (FBAR)

We will file a Foreign Bank and Financial Accounts Report (FBAR) for any financial accounts of more than $10,000 that we hold or have signature or other authority over in a foreign country. We will use the BSA E-Filing System provided on FinCEN's website.

e. Monetary Instrument Purchases (MIL)

We do not issue bank checks or drafts, cashier's checks, money orders, or traveler's checks in the amount of $3,000 or more.

f. Funds Transmittals of $3,000 or More Under the Travel Rule

When we are the transmitter's financial institution in funds of $3,000 or more, we will retain either the original or a copy (e.g., microfilm, electronic record) of the transmittal order. We will also record on the transmittal order the following information: (1) the name and address of the transmitter; (2) if the payment is ordered from an account, the account number; (3) the amount of the transmittal order; (4) the execution date of the

transmittal order; and (5) the identity of the recipient's financial institution. In addition, we will include on the transmittal order as many of the following items of information as are received with the transmittal order: (1) the name and address of the recipient; (2) the account number of the recipient; (3) any other specific identifier of the recipient; and (4) any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order.

We will also verify the identity of the person placing the transmittal order (if we are the transmitting Company), provided the transmittal order is placed in person, and the transmitter is not an established customer of the Company (i.e., a customer of the Company who has not previously maintained an account with us or for whom we have not obtained and maintained a file with the customer's name, address, taxpayer identification number, or, if none, alien identification number or passport number and country of issuance). If a transmitter or recipient is conducting business in person, we will obtain: (1) the person's name and address; (2) the type of identification reviewed and the number of the identification document (e.g., driver's license); and (3) the person's taxpayer identification number (e.g., Social Security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record the lack thereof. If a transmitter or recipient is not conducting business in person, we shall obtain the person's name, address, and a copy or record of the payment method (e.g., check or credit card transaction). In the case of transmitters only, we shall also obtain the transmitter's taxpayer identification number (e.g., Social Security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof. In the case of recipients only, we shall obtain the name and address of the person to which the transmittal was sent.

13. Independent Review of AML Program

Our Company represents and warrants that it shall conduct (or have third party conduct) an independent review of its AML Program at least annually and keep a copy of the report of such independent review report on site for review.

14. AML Recordkeeping

a. Responsibility for Required AML Records and SAR Filing

Our AML Compliance Officer and his or her designee will be responsible for ensuring that AML records are maintained properly and that SARs are filed as required.

In addition, as part of our AML program, we will create and maintain SARs and relevant documentation on customer identity and verification *(See* Section 5 above) and funds transmittals. We will maintain SARs and their accompanying documentation for at least five years. We will keep other documents according to existing BSA and other recordkeeping requirements, including certain SEC rules that require six-year retention periods.

b. SAR Maintenance and Confidentiality

We will hold SARs and any supporting documentation confidential. We 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. We will refuse any subpoena requests for SARs or information that would disclose that a SAR has been prepared or filed and immediately notify FinCEN of any such subpoena requests that the company receives. *See* Section 7 for contact numbers. We will segregate SAR filings and copies of supporting documentation from other Company books and records to avoid disclosing SAR filings. Our AML Compliance Officer will handle all subpoenas or other requests for SARs. We may share information with another financial institution about suspicious transactions in order to determine whether we will jointly file a SAR according to the provisions of Section 3.d. In cases in which Company files a joint SAR for a transaction handled by another financial institution and us, both financial institutions will maintain a copy of the filed SAR.

c. Additional Records

We shall retain either the original or a digital copy or other copy or reproduction of each of the following:

- Each document granting signature or trading authority over each customer's account;

- A record of each remittance or transfer of funds, or of currency, checks, other monetary instruments, investment securities or credit, of more than $10,000 to a person, account or place, outside the US; and

- A record of each receipt of currency, other monetary instruments, checks or investment securities and of each transfer of funds or credit, of more than $10,000 received on any one occasion directly and not through a domestic financial institution, from any person, account, or place outside the US.

15. Clearing/Introducing Company Relationships

We will work closely with our clearing Company to detect money laundering. We will exchange information, records, data, and exception reports as necessary to comply with our contractual obligations and with AML laws. Both our Company and our clearing Company have filed (and kept updated) the annual certifications required for such information sharing, which can be found on FinCEN's website. As a general matter, we will obtain and use the following exception reports offered by our clearing Company to monitor customer activity. We will provide our clearing Company with proper customer identification and due diligence information as required to monitor customer transactions successfully. We have discussed how each Company will apportion customer and transaction functions and how we will share information and set forth our understanding in a written document. We understand that the apportionment of functions will not relieve either of us from our independent obligation to comply with AML laws, except as specifically allowed under the BSA and its implementing regulations.

16. Training Programs

We will develop ongoing employee training under the leadership of the AML Compliance Person and senior management. Our training will occur on at least an annual basis. It will be based on our Company's size, customer base, and 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 SARs); (3) what employees' roles are in the Company's compliance efforts and how to perform them; (4) the Company's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the BSA.

We will develop training in our Company, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos. We will maintain records to show the persons trained, the dates of training, and the subject matter of their training.

We will review our operations to see if certain employees, such as compliance, margin, and corporate security, require additional specialized training. Our written procedures will be updated to reflect any such changes.

17. Monitoring Employee Conduct and Accounts

We will subject employee accounts to the same AML procedures as customer accounts under the supervision of the AML Compliance Person. The AML Compliance Person's accounts will be reviewed by AML Officer. We will also review the AML performance of supervisors as part of their annual performance review.

18. Confidential Reporting of AML Non-Compliance (Whistle-blower protection))

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

19. Additional Risk Areas

The Company has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above. The major additional areas of risk include anti-corruption and trade control compliance.

20. Senior Manager Approval

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

Attachment A – Restricted Activities List

PROHIBITED ACTIVITIES

THE FOLLOWING CATEGORIES OF ACTIVITIES, BUSINESS PRACTICES, AND SALE ITEMS ARE BARRED IN CONNECTION WITH COOPER BLAZER:

- CONDUCTING OR FACILITATING MONEY-LAUNDERING OR TERRORIST FINANCING
- TRANSACTING COUNTERFEIT PRODUCTS OR ANY PRODUCT OR SERVICE THAT INFRINGES UPON THE COPYRIGHT TRADEMARK, OR TRADE SECRETS OF ANY THIRD PARTY
- TRANSACTING STOLEN GOODS
- TRANSACTING NARCOTICS, CONTROLLED SUBSTANCES, PRESCRIPTION AND PHARMACEUTICAL SERVICES, DRUG PARAPHERNALIA, OR ANY SUBSTANCES DESIGNED TO MIMIC ILLEGAL DRUGS
- CERTAIN ILLICIT GAMBLING ACTIVITY
- EXTORTION, BLACKMAIL, OR EFFORTS TO INDUCE UNEARNED PAYMENTS
- UNLICENSED SALE OF FIREARMS AND CERTAIN WEAPONS
- ENGAGING IN DECEPTIVE MARKETING PRACTICES
- DEFRAUDING COOPER BLAZER BY PROVIDING FALSE, INACCURATE, OR MISLEADING INFORMATION
- ANY BUSINESS THAT VIOLATES ANY LAW, STATUTE, ORDINANCE OR REGULATION

Attachment B – Money Laundering Risk Assessment

The National Money Laundering Risk Assessment

The 2022 National Money Laundering Risk Assessment ("NMLRA") identifies the money laundering risks that are of priority concern to the United States. The underlying concepts for the risk assessment contained in the NMLRA are:
(i) threats (the predicate crimes associated with money laundering); (ii) vulnerabilities (the opportunities that facilitate money laundering); and
(iii) risk (the synthesis of threat, vulnerability and consequence).

a. Threats

The NMLRA risk methodology begins with the concept of a threat being the predicate crime that must occur before the need to launder money arises. This can be thought of as the WHY behind the need for money laundering. The NMLRA further states that money laundering is a necessary component of almost all profit-generating crimes and lists fraud and drug trafficking as the two crimes generating the majority of proceeds that necessitate money laundering. Within the world of fraud, the NMLRA highlights identity theft as a growing and expanding area of criminal activity. Within drug trafficking, the NMLRA pays special attention to the dominance of Mexican- based criminal organizations. The NMLRA highlights other predicate crimes, including human smuggling, organized crime, and corruption of government officials.

From its direct experience, Cooper Blazer would add the following crimes to the list of specific threats: online gambling; marijuana-related businesses that may be legal on a state level but remain illegal on the US federal level; and unlicensed Money Services Businesses ("MSBs").

Cooper Blazer's Controls Against Threats

To address the specific threats listed above, Cooper Blazer has implemented the following controls:

- Cooper Blazer maintains a list of restricted activities that includes money laundering and the facilitation thereof in general and many of the specific crimes listed above, including operating as an unlicensed money transmitter, gambling activities, and drug trafficking. All Cooper Blazer counterparties must confirm that they will not conduct business with Cooper Blazer, on the counterparties' behalf or the behalf of a third party, in connection with any of the listed restricted activities. The Restricted Activities List is included in Attachment A.

- As part of its Counterparty Due Diligence process, Cooper Blazer collects information on prospective counterparties and uses third-party services to help discover any known connections to crime. Cooper Blazer will also use general internet-based searches for the same purpose. Cooper Blazer's AML Officer will then evaluate any connections to criminal activity, and a decision will be made as to whether or not to approve the prospective counterparty.

- Prior to entering into transactions with new counterparties, Cooper Blazer utilizes the application/onboarding process of its vendor(s) to prevent identity fraud, among other threats and risks, and to avoid conducting business with persons engaged in money laundering or terrorist financing.

- To address the specific threat of unlicensed MSBs, please see the specific section in this document covering unlicensed MSBs.

b. Vulnerabilities

The next step in the NMLRA risk methodology is the concept of vulnerability or the opportunities that allow for money laundering to occur. This can be thought of as the HOW money laundering occurs. The NMLRA states that the breadth of products and services in the United States financial industry creates a complex, dynamic environment in which illegitimate actors are continuously seeking opportunities. The main money laundering methods identified are:

Vulnerability Identified	**Cooper Blazer Controls**	**Residual Vulnerability**

Use of cash and monetary instruments in amounts under regulatory recordkeeping and reporting thresholds	Cooper Blazer does not accept or deal with physical cash. Instead, Cooper Blazer accepts and deals in currency through the use of money wires and the traditional	Low

	banking sector. Additionally, unless otherwise approved, Cooper Blazer's Average transaction size is $ 200 USD. Therefore, the concern of structuring is controlled by these two facts as the Company's banking partners will file Currency Transaction Reports for nearly all transactions involving Cooper Blazer. Additionally, Cooper Blazer retains records on every currency transaction, regardless of size, and stands ready to assist in filing Suspicious Activity Reports when appropriate.	
Opening bank accounts using nominees to disguise the identity of the individuals who control the accounts	Cooper Blazer's control here relies on the strength of its onboarding process and Customer Due Diligence. Please see the related section of this document for more information on these efforts.	Medium
Creating legal entities Without accurate information about the identity of the beneficial owner	Cooper Blazer's control here relies on the strength of its onboarding process and Customer Due Diligence. For purposes of identifying beneficial owners, Cooper Blazer uses the definition of beneficial owner contained in FinCEN's Customer Due Diligence Requirements for Financial Institutions	Medium

	released on May 11, 2016. Please see the related section of this document for more information on these efforts.	
Misuse of products and services resulting from deficient compliance with Anti-money laundering obligations	Cooper Blazer's control against this vulnerability is two-fold. The first iseducation and training. In thistime, Cooper Blazer has become very educated on how the banking sector operates. Additionally, Cooper Blazeris committed to Company-wide training on AML issues. Second, Cooper Blazer's transaction monitoring efforts, described in detail in a latter section of this document, is designed to catch any association of its counterparties to known illicit marketplaces, which Cooper Blazer would consider to be a misuseof its services.	Medium
Merchants and financial institutions wittingly facilitatingillicitactivity	Cooper Blazer addresses this vulnerability as a financial institution itself through taking its AML responsibilities with the utmost seriousness and by	Medium

	having an AML programin place. Cooper Blazer expects its counterparties to have a serious AML program and requests evidence of such.	

The NMLRA states that establishing and maintaining an effective customer identification program (CIP) is a key control in addressing vulnerabilities.

c. Risks

The last component of the NMLRA is the concept of risk, or the synthesis of the concepts of threat and vulnerability multiplied by the harm or consequence. Risk represents a summary judgment of all other components. Specific risks listed include:

Risk	**Cooper Blazer Controls**	**Residual Risk**
Widespread use of cash, making it difficult for authorities to differentiate between licit and illicit use and movement of banknotes	As noted above, Cooper Blazer does not accept cash as payment or collateral.	Low
Structured transactions below applicable thresholds to avoid reporting and recordkeeping obligations	As noted above, Cooper Blazer does not accept or deal with physical cash. Instead, Cooper Blazer's involvement with currency involves money wires and the traditional banking sector. Additionally, unless otherwise approved, Cooper Blazer's average transaction size is $200 USD. Therefore, the concern of structuring is controlled by these two facts as the Company's banking partners will file Currency Transaction Reports for	Low

	nearly all transactions involving Cooper Blazer. Additionally, Cooper Blazer retains records on every currency transaction, regardless of size, and stands ready to assist filing Suspicious Activity Reports when appropriate.	
A variation on routine structuring is the misuse of currency deposits or interstate funnel accounts, which involves using an account at a bank with branches nationwide to make structured deposits in one or more geographic locations and then structured withdrawals in the state where the account was opened. The typical interstate funnel account is held by a nominee in one state and receives regular cash deposits at branch locations in other states.	Cooper Blazer's control against this risk comes in its onboarding process, which requires potential counterparties to identify whether they regularly engage in cash trades. A positive response will be evaluated along with other factors (such as if the counterparty is a registered MSB and has an AML program).	Low
Individuals and entities that disguise the nature, purpose, ownership, and control of accounts	As previously stated, Cooper Blazer's control here relies on the strength of its onboarding process and Customer Due Diligence. Please see the related section of this document for more information on these efforts.	Medium
Occasional AML compliance deficiencies, which are an inevitable	Cooper Blazer addresses this risk as a financial institution itself through	Medium

consequence of a financial system with hundreds of thousands of locations for financial services	taking its AML responsibilities with the utmost seriousness and by having an AML program in place.	
Complicit violators within financial institutions; and complicit merchants, particularly wholesalers who facilitate trade-based money laundering, and financial services providers	Cooper Blazer addresses this risk by having an expectation that fellow financial institutions, including MSBs, have a serious AML program and requesting evidence of such.	Medium

1. Bank Secrecy Act/Anti-Money Laundering Examination Manual for MSBs

In 2008, FinCEN produced the Bank Secrecy Act/Anti-Money Laundering Examination Manual for MSBs (the "MSB Manual"). Cooper Blazer finds the document helpful for assessing risk. Specifically, the MSB Manual provides the following components to a risk assessment: product risk, customer risk, geographic risk, and operational risk.

a. Product Risk

The MSB Manual states that "offering certain products and services, such as those that provide customers with greater anonymity or involve handling high volumes of currency or currency equivalents, may present a higher risk of money laundering." Consequently, Cooper Blazer is committed to taking all possible measures to mitigate this increased risk. For instance, Cooper Blazer refrains from conducting transactions with unknown parties and requires all counterparties to undergo an onboarding process designed to fulfill its Customer Due Diligence obligations. Additionally, the entire anti-money laundering (AML) program is designed to address the risk associated with transaction execution.

Residual Risk: Medium

b. Customer Risk

Capturing the full spectrum of Cooper Blazer's diverse customer base is undeniably challenging. However, the company has implemented several controls to mitigate the inherent risks associated with its customers. To effectively address these risks, Cooper Blazer has established robust customer due diligence (CDD) procedures, which include implementing Know Your Customer (KYC) requirements. These procedures involve verifying the identity of customers, evaluating their risk profiles, and monitoring transactions for any suspicious activities. In addition, Cooper Blazer ensures the establishment of effective internal controls, conducts ongoing employee training, and maintains compliance with relevant anti-money

laundering (AML) laws and regulations.

c. Geographic Risk

The majority of Cooper Blazer's counterparties are United States persons and entities. As part of its onboarding process, Cooper Blazer uses third-party services to screen the prospective counterparty against the various watch lists, including the Specially Designated Nationals List, OFAC sanctions lists, and countries and territories identified as non-cooperative by the Financial Action Task Force.

d. Operational Risk

The MSB Manual defines operational risk as the risk that an institution will fail to detect or prevent money laundering or terrorist financing as a result of inadequate processes or systems or as a result of human failure. The MSB Manual provides the following components of operational risk:

Operational Risk	**Cooper Blazer Control**	**Residual Risk**
Use of Systems to process transactions that use transactional dollar limitations	Cooper Blazer enforces a transaction limit ranging from $200 to $500, with the lowest fee incentive set at 0.01%, in order to mitigate the risks associated with higher remittance amounts.	Low

Frequency of employee turnover	Employee turnover is not yet applicable to Cooper Blazer based on the entity's recent formation.	Low
Recordkeeping system	Cooper Blazer has partnered with third party vendors on its onboarding platform. The platform houses detailed records concerning every new counterparty onboarded to Cooper Blazer.	Low
Activities of institution	Cooper Blazer leverages the onboarding process ofthird party vendors	Medium
Institution's business structure and business plan	Cooper Blazer has a pretty simple business plan and structure in which it routes transactions between sender and receiver on its platform fora transaction fee. Most of Cooper Blazer' potential business risk arises from the way it manages risk from both a counterparty and collateral perspective.	Medium

Involvement of senior management in BSA matters	Cooper Blazer's CCO and CEO meet regularly to discuss various compliance matters, including BSA matters.	Low
Institution's agency relationships	Cooper Blazer does not have any agency relationships.	Low

Attachment C – Risk Scorecard and EDD Risk Scorecard

Cooper Blazer has developed a Risk Scorecard (please see Appendix A below) in which to assess potential counterparties during the onboarding process. Cooper Blazer has modeled the Risk Scorecard on risk assessment principles established by The Wolfsberg Group of International Financial Institutions.

The Risk Scorecard is designed to account for the specifics of Cooper Blazer's business, information collected through the New Applicant Profile, and any relevant regulatory guidance. The Risk Scorecard should not be considered a fixed document, but should evolve and change as needed.

The Risk Scorecard shall be used to determine whether a counterparty triggers Enhanced Due Diligence ("EDD"). Specifically, any counterparty with a qualifying score shall qualify for Enhanced Due Diligence.

Appendix A: CDD Score Card

CDD Score Card			
Risk Attribute Classification	**Assigned Scores**	**Min-Max**	**Weight**
Anticipated Transaction Amount	<$1K	0-30	Low
	>$3K		
Actual Transaction Amount	<$3K	0-30	High
	>$10K		
Countries: US vs. Foreign	10 or 30	0-30	Mod
SAR Filings	0=No, 30=Yes	0-30	Mod
Overall Composite Risk Score	**Min 30 to Max 120**	**30-120**	**Low-High**
Low=30 to ≤70	Moderate=71 to ≤99	High=<100	