

# "A" Spine Investments Ltd Anti-Money Laundering (AML) Program: Compliance and Supervisory Procedures

---

UPDATED AS OF MARCH 10, 2022

## **1. Firm Policy**

It is the policy of the firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the Bank Secrecy Act (BSA) and its implementing regulations.

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.

Although cash is rarely deposited into securities accounts, the securities industry is unique in that it can be used to launder funds obtained elsewhere, and to generate illicit funds within the industry itself through fraudulent activities. Examples of types of fraudulent activities include insider trading, market manipulation, ponzi schemes, cybercrime and other investment-related fraudulent activity.

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

## **2. AML Compliance Person Designation and Duties**

The firm has designated UP-X as its Anti-Money Laundering Program Compliance Person "Head of information security service", with full responsibility for the firm's AML program. UP-X has a working knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge and training. The duties of the AML Compliance Person will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees, and. The AML Compliance Person will also ensure that the firm keeps and maintains all of the required AML records and will ensure that Suspicious Activity Reports (SARs) are filed with the Financial Crimes Enforcement Network (FinCEN) when appropriate. The AML Compliance Person is vested with full responsibility and authority to enforce the firm's AML program.

We 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. UP-X 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 we 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, 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 the receipt of 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 that 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 the procedure described by our company's internal regulations. 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 in itself 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 as well as 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. 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. UP-X will ensure that the firm files with FinCEN an initial notice before any sharing occurs and annual notices thereafter. We will use the notice form found at [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 that 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 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 firm'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 SARs by Broker-Dealers and Other Financial Institutions**

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 jointly a SAR.

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 (*e.g.*, because the SAR concerns the other broker-dealer or one of its employees), 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, UP-X 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 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 on a regular basis and subscribe to receive any available updates when they occur. With respect to the SDN list, we may also access that list through various software programs to ensure speed and accuracy.

#### **5. Customer Identification Program**

We do not open or maintain customer accounts within the meaning of 31 CFR 1023.100, in that we do not establish formal relationships with “customers” for the purpose of effecting transactions in securities. If in the future the firm elects to open customer accounts or to establish formal relationships with customers for the purpose of effecting transactions in securities, we will first establish, document and ensure the implementation of appropriate CIP procedures.

We will 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 U.S., and status or verification of the authenticity of a government agency or department).

**a. Required Customer Information**

*Prior* to opening an account, UP-X 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 U.S. 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, our firm will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, our AML Compliance Person will be notified so that we can determine whether we should report the situation to FinCEN on a SAR.

**c. Verifying Information**

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know 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. UP-X will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

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 the use of documentary evidence by using the non-documentary means described below whenever necessary. We may also use non-documentary means, if we are still uncertain about whether we know the true identity of the customer. In verifying the information, we will consider whether the identifying information that we receive, such as the customer's name, street address, zip code, telephone number (if provided), date of birth and Social Security number, allow us to determine that we have 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 safeguard, 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.

We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. If, 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 source;
- Checking references with other financial institutions; or
- Obtaining a financial statement.

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) the firm is unfamiliar with the documents the customer presents for identification verification;
- (3) the customer and firm do not have face-to-face contact; and
- (4) there are other circumstances that increase the risk that the firm will be unable to verify the true identity of the customer 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, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, we will, after internal consultation with the firm's AML Compliance Person, file a SAR in accordance with applicable laws and regulations.

We recognize that the risk that we 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 has been designated by the U.S. 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. We will also take the following additional measures that may be used to obtain information about the identity of the individuals associated with the customer when standard documentary methods prove to be insufficient.

#### **d. Lack of Verification**

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (1) not open an account; (2) impose terms under which a customer may conduct transactions while we attempt 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 file a SAR in accordance with applicable laws and regulations.

#### **e. Recordkeeping**

We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We will keep records containing a

description of any document that we 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 the identity of a customer. 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 we receive 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 provide notice to customers that the firm is requesting information from them to verify their identities, as required by federal law. We will use the following method to provide notice to customers: E-mail, Telegram messages, VK, FB

**Important Information About Procedures for Opening a New Account**

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.

**What this means for you: When you 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 U.S.C. § 5318(h), and is regulated by a federal functional regulator; and
- when the other financial institution has entered into a contract with our firm 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**

We do not open or maintain accounts for legal entity customers within the meaning of 31 CFR 1010.230. If in the future the firm elects to open accounts for legal entity customers, we will first establish, document and ensure the implementation of appropriate CDD procedures.

#### **a. Identification and Verification of Beneficial Owners**

At the time of opening an account for a legal entity customer, head of information security service 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 U.S. persons), or one or more of the following: a passport number and country of issuance, or other similar identification number, 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 for the purpose of developing a customer risk profile.

**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. Due Diligence and Enhanced Due Diligence Requirements for Correspondent Accounts of Foreign Financial Institutions**

**a. Due Diligence for Correspondent Accounts of Foreign Financial Institutions**

We have reviewed our accounts and we do not have, nor do we intend to open or maintain, correspondent accounts for foreign financial institutions

**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 U.S. 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 to 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 a payable-through account (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 the identity of each owner 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.

## **8. Due Diligence and Enhanced Due Diligence Requirements for Private Banking Accounts/Senior Foreign Political Figures**

We do not open or maintain private banking accounts.

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

We do not maintain any accounts (including correspondent accounts) with any foreign jurisdiction or financial institution. However, 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, we understand that we must read FinCEN's final rule and follow any prescriptions or prohibitions contained in that rule.

## **10. 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.) Monitoring will be conducted through the following methods: automatic moderation of similar transactions, visual moderation. The customer risk profile will serve as a baseline for assessing potentially suspicious activity. The AML Compliance Person or his or her designee head of security will be responsible for this monitoring, will review any activity that our monitoring system detects, 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.

We will conduct the following reviews of activity that our monitoring system detects: manual monitoring, automatic monitoring. We will document our monitoring and reviews as follows: keeping historicity in our databases. The AML Compliance Person or his or her designee will conduct an appropriate investigation and review relevant information from internal or third-party sources before a SAR is filed.

#### **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 U.S. Attorney's office (*insert contact number*), local FBI office (*insert contact number*) and local SEC office (*insert contact number*) (to voluntarily report such violations to the SEC in addition to contacting the appropriate law enforcement authority). If we notify the appropriate law enforcement authority of any such activity, we must still file a timely a SAR.

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

#### **Potential Red Flags in Customer Due Diligence and Interactions with Customers**

- The customer provides the firm with unusual or suspicious identification documents that cannot be readily verified or are inconsistent with other statements or documents that the customer has provided. Or, the customer provides information that is inconsistent with other available information about the customer. This indicator may apply to account openings and to interaction subsequent to account opening.
- The customer is reluctant or refuses to provide the firm with complete customer due diligence information as required by the firm's procedures, which may include information regarding the nature and purpose of the customer's business, prior financial relationships, anticipated account activity, business location and, if applicable, the entity's officers and directors.

- The customer refuses to identify a legitimate source of funds or information is false, misleading or substantially incorrect.
- The customer is domiciled in, doing business in or regularly transacting with counterparties in a jurisdiction that is known as a bank secrecy haven, tax shelter, high-risk geographic location (*e.g.*, known as a narcotics producing jurisdiction, known to have ineffective AML/Combating the Financing of Terrorism systems) or conflict zone, including those with an established threat of terrorism.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer has no discernable reason for using the firm's service or the firm's location (*e.g.*, the customer lacks roots to the local community or has gone out of his or her way to use the firm).
- The customer has been rejected or has had its relationship terminated as a customer by other financial services firms.
- The customer's legal or mailing address is associated with multiple other accounts or businesses that do not appear related.
- The customer appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.
- The customer is a trust, shell company or private investment company that is reluctant to provide information on controlling parties and underlying beneficiaries.
- The customer is publicly known or known to the firm to have criminal, civil or regulatory proceedings against him or her for crime, corruption or misuse of public funds, or is known to associate with such persons. Sources for this information could include news items, the Internet or commercial database searches.
- The customer's background is questionable or differs from expectations based on business activities.
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, with no apparent business or other purpose.
- An account is opened by a politically exposed person (PEP),<sup>9</sup> particularly in conjunction with one or more additional risk factors, such as the account being opened by a shell company<sup>10</sup> beneficially owned or controlled by the PEP, the PEP is from a country which has been identified by FATF as having strategic AML regime deficiencies, or the PEP is from a country known to have a high level of corruption.
- An account is opened by a non-profit organization that provides services in geographic locations known to be at higher risk for being an active terrorist threat.<sup>11</sup>
- An account is opened in the name of a legal entity that is involved in the activities of an association, organization or foundation whose aims are related to the claims or demands of a known terrorist entity.<sup>12</sup>

- An account is opened for a purported stock loan company, which may hold the restricted securities of corporate insiders who have pledged the securities as collateral for, and then defaulted on, purported loans, after which the securities are sold on an unregistered basis.
- An account is opened in the name of a foreign financial institution, such as an offshore bank or broker-dealer, that sells shares of stock on an unregistered basis on behalf of customers.
- An account is opened for a foreign financial institution that is affiliated with a U.S. broker-dealer, bypassing its U.S. affiliate, for no apparent business purpose. An apparent business purpose could include access to products or services the U.S. affiliate does not provide.

### **Potential Red Flags in Deposits of Securities**

- A customer opens a new account and deposits physical certificates, or delivers in shares electronically, representing a large block of thinly traded or low-priced securities.
- A customer has a pattern of depositing physical share certificates, or a pattern of delivering in shares electronically, immediately selling the shares and then wiring, or otherwise transferring out the proceeds of the sale(s).
- A customer deposits into an account physical share certificates or electronically deposits or transfers shares that:
  - were recently issued or represent a large percentage of the float for the security;
  - reference a company or customer name that has been changed or that does not match the name on the account;
  - were issued by a shell company;
  - were issued by a company that has no apparent business, revenues or products;
  - were issued by a company whose SEC filings are not current, are incomplete, or nonexistent;
  - were issued by a company that has been through several recent name changes or business combinations or recapitalizations;
  - were issued by a company that has been the subject of a prior trading suspension; or
  - were issued by a company whose officers or insiders have a history of regulatory or criminal violations, or are associated with multiple low-priced stock issuers.
- The lack of a restrictive legend on deposited shares seems inconsistent with the date the customer acquired the securities, the nature of the transaction in which the securities were acquired, the history of the stock or the volume of shares trading.
- A customer with limited or no other assets at the firm receives an electronic transfer or journal transfer of large amounts of low-priced, non-exchange-listed securities.

- The customer's explanation or documents purporting to evidence how the customer acquired the shares does not make sense or changes upon questioning by the firm or other parties. Such documents could include questionable legal opinions or securities purchase agreements.
- The customer deposits physical securities or delivers in shares electronically, and within a short timeframe, requests to journal the shares into multiple accounts that do not appear to be related, or to sell or otherwise transfer ownership of the shares.
- Seemingly unrelated clients open accounts on or at about the same time, deposit the same low-priced security and subsequently liquidate the security in a manner that suggests coordination.

### **Potential Red Flags in Securities Trading**

- The customer, for no apparent reason or in conjunction with other "red flags," engages in transactions involving certain types of securities, such as penny stocks, Regulation "S" stocks and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
- There is a sudden spike in investor demand for, coupled with a rising price in, a thinly traded or low-priced security.
- The customer's activity represents a significant proportion of the daily trading volume in a thinly traded or low-priced security.
- A customer buys and sells securities with no discernable purpose or circumstances that appear unusual.
- Individuals known throughout the industry to be stock promoters sell securities through the broker-dealer.
- A customer accumulates stock in small increments throughout the trading day to increase price.
- A customer engages in pre-arranged or other non-competitive securities trading, including wash or cross trades, with no apparent business purpose.
- A customer attempts to influence the closing price of a stock by executing purchase or sale orders at or near the close of the market.
- A customer engages in transactions suspected to be associated with cyber breaches of customer accounts, including potentially unauthorized disbursements of funds or trades.

- A customer engages in a frequent pattern of placing orders on one side of the market, usually inside the existing National Best Bid or Offer (NBBO), followed by the customer entering orders on the other side of the market that execute against other market participants that joined the market at the improved NBBO (activity indicative of “spoofing”).
- A customer engages in a frequent pattern of placing multiple limit orders on one side of the market at various price levels, followed by the customer entering orders on the opposite side of the market that are executed and the customer cancelling the original limit orders (activity indicative of “layering”).
- Two or more unrelated customer accounts at the firm trade an illiquid or low-priced security suddenly and simultaneously.
- The customer makes a large purchase or sale of a security, or option on a security, shortly before news or a significant announcement is issued that affects the price of the security.
- The customer is known to have friends or family who work at or for the securities issuer, which may be a red flag for potential insider trading or unlawful sales of unregistered securities.
- The customer’s purchase of a security does not correspond to the customer’s investment profile or history of transactions (*e.g.*, the customer may never have invested in equity securities or may have never invested in a given industry, but does so at an opportune time) and there is no reasonable explanation for the change.
- The account is using a master/sub structure, which enables trading anonymity with respect to the sub-accounts’ activity, and engages in trading activity that raises red flags, such as the liquidation of microcap issuers or potentially manipulative trading activity.
- The firm receives regulatory inquiries or grand jury or other subpoenas concerning the firm’s customers’ trading.
- The customer engages in a pattern of transactions in securities indicating the customer is using securities to engage in currency conversion. For example, the customer delivers in and subsequently liquidates American Depositary Receipts (ADRs) or dual currency bonds for U.S. dollar proceeds, where the securities were originally purchased in a different currency.
- The customer engages in mirror trades or transactions involving securities used for currency conversions, potentially through the use of offsetting trades.

- The customer appears to buy or sell securities based on advanced knowledge of pending customer orders.

### **Potential Red Flags in Money Movements**

- The customer attempts or makes frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies and procedures relating to the deposit of cash and cash equivalents.
- The customer "structures" deposits, withdrawals or purchases of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements, and may state directly that they are trying to avoid triggering a reporting obligation or to evade taxing authorities.
- The customer seemingly breaks funds transfers into smaller transfers to avoid raising attention to a larger funds transfer. The smaller funds transfers do not appear to be based on payroll cycles, retirement needs, or other legitimate regular deposit and withdrawal strategies.
- The customer's account shows numerous currency, money order (particularly sequentially numbered money orders) or cashier's check transactions aggregating to significant sums without any apparent business or lawful purpose.
- The customer frequently changes bank account details or information for redemption proceeds, in particular when followed by redemption requests.
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
- Wire transfers are made in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Incoming payments are made by third-party checks or checks with multiple endorsements.
- Outgoing checks to third parties coincide with, or are close in time to, incoming checks from other third parties.
- Payments are made by third party check or money transfer from a source that has no apparent connection to the customer.
- Wire transfers are made to or from financial secrecy havens, tax havens, high-risk geographic locations or conflict zones, including those with an established presence of terrorism.

- Wire transfers originate from jurisdictions that have been highlighted in relation to black market peso exchange activities.
- The customer engages in transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (*e.g.*, countries designated by national authorities, such as FATF, as non-cooperative countries and territories).
- The parties to the transaction (*e.g.*, originator or beneficiary) are from countries that are known to support terrorist activities and organizations.
- Wire transfers or payments are made to or from unrelated third parties (foreign or domestic), or where the name or account number of the beneficiary or remitter has not been supplied.
- There is wire transfer activity that is unexplained, repetitive, unusually large, shows unusual patterns or has no apparent business purpose.
- The securities account is used for payments or outgoing wire transfers with little or no securities activities (*i.e.*, account appears to be used as a depository account or a conduit for transfers, which may be purported to be for business operating needs).
- Funds are transferred to financial or depository institutions other than those from which the funds were initially received, specifically when different countries are involved.
- The customer engages in excessive journal entries of funds between related or unrelated accounts without any apparent business purpose.
- The customer uses a personal/individual account for business purposes or vice versa.
- A foreign import business with U.S. accounts receives payments from outside the area of its customer base.
- There are frequent transactions involving round or whole dollar amounts purported to involve payments for goods or services.
- Upon request, a customer is unable or unwilling to produce appropriate documentation (*e.g.*, invoices) to support a transaction, or documentation appears doctored or fake (*e.g.*, documents contain significant discrepancies between the descriptions on the transport document or bill of lading, the invoice, or other documents such as the certificate of origin or packing list).

- The customer requests that certain payments be routed through nostro<sup>14</sup> or correspondent accounts held by the financial intermediary instead of its own accounts, for no apparent business purpose.
- Funds are transferred into an account and are subsequently transferred out of the account in the same or nearly the same amounts, especially when the origin and destination locations are high-risk jurisdictions.
- A dormant account suddenly becomes active without a plausible explanation (*e.g.*, large deposits that are suddenly wired out).
- Nonprofit or charitable organizations engage in financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- There is unusually frequent domestic and international automated teller machine (ATM) activity.
- A person customarily uses the ATM to make several deposits into a brokerage account below a specified BSA/AML reporting threshold.
- Many small, incoming wire transfers or deposits are made using checks and money orders that are almost immediately withdrawn or wired out in a manner inconsistent with the customer's business or history; the checks or money orders may reference in a memo section "investment" or "for purchase of stock." This may be an indicator of a Ponzi scheme or potential funneling activity.
- Wire transfer activity, when viewed over a period of time, reveals suspicious or unusual patterns, which could include round dollar, repetitive transactions or circuitous money movements.

### **Potential Red Flags in Insurance Products**

- The customer cancels an insurance contract and directs that the funds be sent to a third party.
- The customer deposits an insurance annuity check from a cancelled policy and immediately requests a withdrawal or transfer of funds.
- The customer cancels an annuity product within the free-look period. This could be a red flag if accompanied with suspicious indicators, such as purchasing the annuity with several sequentially numbered money orders or having a history of cancelling annuity products during the free-look period.

- The customer opens and closes accounts with one insurance company, then reopens a new account shortly thereafter with the same insurance company, each time with new ownership information.
- The customer purchases an insurance product with no concern for the investment objective or performance.

### **Other Potential Red Flags**

- The customer is reluctant to provide information needed to file reports to proceed with the transaction.
- The customer exhibits unusual concern with the firm's compliance with government reporting requirements and the firm's AML policies.
- The customer tries to persuade an employee not to file required reports or not to maintain the required records.
- Notifications received from the broker-dealer's clearing firm that the clearing firm had identified potentially suspicious activity in customer accounts. Such notifications can take the form of alerts or other concern regarding negative news, money movements or activity involving certain securities.
- Law enforcement has issued subpoenas or freeze letters regarding a customer or account at the securities firm.
- The customer makes high-value transactions not commensurate with the customer's known income or financial resources.
- The customer wishes to engage in transactions that lack business sense or an apparent investment strategy, or are inconsistent with the customer's stated business strategy.
- The stated business, occupation or financial resources of the customer are not commensurate with the type or level of activity of the customer.
- The customer engages in transactions that show the customer is acting on behalf of third parties with no apparent business or lawful purpose.
- The customer engages in transactions that show a sudden change inconsistent with normal activities of the customer.
- Securities transactions are unwound before maturity, absent volatile market conditions or other logical or apparent reason.
- The customer does not exhibit a concern with the cost of the transaction or fees (*e.g.*, surrender fees, or higher than necessary commissions).

- A borrower defaults on a cash-secured loan or any loan that is secured by assets that are readily convertible into currency.
- There is an unusual use of trust funds in business transactions or other financial activity.

### **c. Responding to Red Flags and Suspicious Activity**

When an employee of the firm detects any red flag, or other activity that may be suspicious, he or she will notify head of security. Under the direction of the AML Compliance Person, the firm will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or filing a SAR.

## **11. 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 firm involving \$5,000 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 firm 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. It is our policy 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 a SAR, and we will collect and maintain supporting documentation as required by the BSA regulations. We 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. If no suspect is identified on the date of initial detection, we may delay filing the SAR 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.

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. 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 upon request.

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 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 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**

*We file a currency transaction report (CTR) for each deposit, withdrawal, exchange of currency, or other payment or transfer by, through or to the firm that involves a transaction in currency of more than \$10,000 or for multiple transactions in currency of more than \$10,000*

We will file a Foreign Bank and Financial Accounts Report (FBAR) for any financial accounts of more than \$10,000 that we hold, or for which we 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**

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 firm), provided the transmittal order is placed in person and the transmitter is not an established customer of the firm (*i.e.*, a customer of the firm 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 method of payment (*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.

## **12. AML Recordkeeping**

### **a. Responsibility for Required AML Records and SAR Filing**

Our AML Compliance Person 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, our firm will create and maintain SARs, CTRs, CMIRs, FBARs, 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 (*e.g.*, Exchange Act Rule 17a-4(a) requiring firms to preserve for a period of not less than six years, all records required to be retained by Exchange Act Rule 17a-3(a)(1)-(3), (a)(5), and (a)(21)-(22) and Exchange Act Rule 17a-4(e)(5) requiring firms to retain for six years account record information required pursuant to Exchange Act Rule 17a-3(a)(17)).

### **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 for information that would disclose that a SAR has been prepared or filed and immediately notify FinCEN of any such subpoena requests that we receive. *See* Section 11 for contact numbers. We will segregate SAR filings and copies of supporting documentation from other firm books and records to avoid disclosing SAR filings. Our AML Compliance Person 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 we file a joint SAR for a transaction that has been handled both by us and another financial institution, both financial institutions will maintain a copy of the filed SAR.

### **c. Additional Records**

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

- A record of each extension of credit in an amount in excess of \$10,000, except an extension of credit secured by an interest in real property. The record shall contain the name and address of the person to whom the extension of credit is made, the amount thereof, the nature or purpose thereof and the date thereof;
- A record of each advice, request or instruction received or given regarding any transaction resulting (or intended to result and later canceled if such a record is normally made) in the transfer of currency or other monetary instruments, funds, checks, investment securities or credit, of more than \$10,000 to or from any person, account or place outside the U.S.;
- A record of each advice, request or instruction given to another financial institution (which includes broker-dealers) or other person located within or without the U.S., regarding a transaction intended to result in the transfer of funds, or of currency, other monetary instruments, checks, investment securities or credit, of more than \$10,000 to a person, account or place outside the U.S.;
- Each document granting signature or trading authority over each customer's account;
- Each record described in Exchange Act Rule 17a-3(a): (1) (blotters), (2) (ledgers for assets and liabilities, income, and expense and capital accounts), (3) (ledgers for cash and margin accounts), (4) (securities log), (5) (ledgers for securities in transfer, dividends and interest received, and securities borrowed and loaned), (6) (order tickets), (7) (purchase and sale tickets), (8) (confirms), and (9) (identity of owners of cash and margin accounts);
- 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 U.S.; 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 U.S.

### **13. Clearing/Introducing Firm Relationships**

We will work closely with our clearing firm to detect money laundering. We will exchange information, records, data and exception reports as necessary to comply with

AML laws. Both our firm and our clearing firm have filed (and kept updated) the necessary annual certifications 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 firm in order to monitor customer activity and we will provide our clearing firm with proper customer identification and due diligence information as required to successfully monitor customer transactions. We have discussed how each firm 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.

## **14. 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 firm's size, its customer base, 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 SARs); (3) what employees' roles are in the firm's compliance efforts and how to perform them; (4) the firm's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the BSA.

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

## **15. Program to Independently Test AML Program**

### **a. Staffing**

The testing of our AML program will be performed at least annually (on a calendar year basis), personnel of our firm. Their his qualifications include a working knowledge of applicable requirements under the BSA and its implementing regulations. To ensure that

they he remain independent, we will separate their his functions from other AML activities. Independent testing will be performed more frequently if circumstances warrant.

**b. Evaluation and Reporting**

After we have completed the independent testing, staff will report its findings to senior management. We will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved.

**16. 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. We will also review the AML performance of supervisors, as part of their annual performance review. The AML Compliance Person's accounts will be reviewed by product Owner

**17. Confidential Reporting of AML Non-Compliance**

Employees will promptly report any potential violations of the firm'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 chairman of the board of directors. Such reports will be confidential, and the employee will suffer no retaliation for making them.

**18. Additional Risk Areas**

The firm 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 attempts to replenish accounts from unverified accounts. Additional procedures to address these major risks are manual validation of new users. The firm 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 attempts to replenish accounts from unverified accounts. Additional procedures to address these major risks are manual validation of new users.

**19. Senior Manager Approval**

Senior management has approved this AML compliance program in writing as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of

the BSA and the implementing regulations under it. This approval is indicated by signatures below.

Signed:

Title: David Chan

Date: 2021-01-21

A handwritten signature in blue ink, consisting of several stylized, connected strokes that are difficult to decipher as specific letters.