Cresta Westhall LLP

Anti-Money Laundering Compliance Program

Table of Contents

These anti-money laundering compliance procedures were approved by Doug Fulton, CCO. These procedures are effective from the date approved until the date of their authorized revision, update or replacement (see below).

Authorized Approval Signature:  _____ Date: March 15, 2023

Anti-Money Laundering Compliance Program

Name of Supervisor:	Designated AML Program Supervisor: Richard Pound Chief Compliance Officer: Doug Fulton Designated Principals (see WSP Manual)
Frequency of Review:	Daily, in the course of normal account/RR supervision; Immediate review of P-SARs and SAR-SFs
How Conducted:	In accordance with Program described below, including: Review of Preliminary (internal) Suspicious Activity Reports (P-SAR) Review transaction records related to suspicious activity Review of client files for names/entities on OFAC or SEC Control List File AML contact information with FINRA; review information periodically and file changes as necessary.
How Documented:	Notes to customer files Preliminary Suspicious Activity Reports P-SAR Review Form Account documentation Necessary filed reports (Currency Transaction Report; Suspicious Activity Report by the Securities and Futures Industry, etc.) Forward transmittal information when necessary (see below)
3010 Checklist:	Conduct FINRA Consolidated Rule 3310, IM-3011-1, IM-3011-2; SEC Rule 17a-8, USA PATRIOT Act (including among others, Sections 312, 314, 326, and 352); Bank Secrecy Act; NTM's 02-21, 03-34, 06-07
Comments:	

In accordance with FINRA Consolidated Rule 3310, and in an effort to comply with the applicable requirements under the USA PATRIOT Act and the Bank Secrecy Act, Cresta Westhall LLP (the "Company") has established the following policies and procedures for the purpose of attempting to deter and detect money laundering activities by customers. All employees and associated persons of the Company must comply with the applicable provisions under the Bank Secrecy Act and the AML provisions under the USA PATRIOT Act and every employee and associated person of the Company is expected to be familiar with the policies and procedures herein and to make reasonable efforts to comply with them. Failure to do so will result in disciplinary action and possible subsequent termination of employment. Company personnel, in following the enclosed policies, will also assist in detecting and deterring check fraud, ID theft, embezzlement, securities fraud, insider trading and other illegal activities not strictly related to money laundering.

It is the intention of Cresta Westhall LLP, in implementing its Anti-Money Laundering Compliance Program, to meet the requirements of FINRA Consolidated Rule 3310, which states:

> "Each member shall develop and implement a written anti-money laundering program reasonably designed to achieve and monitor the member's compliance with the requirements of the Bank Secrecy Act (31 U.S.C. 5311, *et seq.*), and the implementing regulations promulgated thereunder by the Department of the Treasury. Each member organization's anti-money laundering program must be approved, in writing, by a member of senior management. The anti-money laundering programs required by this Rule shall, at a minimum,
>
> (a) Establish and implement policies and procedures that can be reasonably expected to detect and cause the reporting

transactions required under 31 U.S.C. 5318(g) and the implementing regulations thereunder;

(b) Establish and implement policies, procedures, and internal controls reasonably designed to achieve compliance with the Bank Secrecy Act and the implementing regulations thereunder;

(c) Provide for annual (on a calendar-year basis) independent testing for compliance to be conducted by member personnel or by a qualified outside party, unless the member does not execute transactions for customers or otherwise hold customer accounts or act as an introducing broker with respect to customer accounts (e.g., engages solely in proprietary trading or conducts business only with other broker-dealers), in which case such "independent testing" is required every two years (on a calendar-year basis). ~~n the case of Cresta Westhall, given it does not execute customer accounts or hold customer monies, the requirement is for this testing to be undertaken every 2 years.~~ Designate and identify to FINRA (by name, title, mailing address, e-mail address, telephone number, and facsimile number) an individual or individuals responsible for implementing and monitoring the day-to-day operations and internal controls of the program (such individual or individuals must be an associated person of the member) and provide prompt notification to FINRA regarding any change in such designation(s); and

(d) Provide ongoing training for appropriate personnel."

Assessment of the Company's business: The Company does not receive or hold customer funds or securities, does not accept currency and does open accounts for customers. The Company's business is limited to assist alternative investment general partners/managers in raising capital on a best efforts basis only. Therefore, while some areas of the regulations may not apply to the Company, given its business, this fact does not diminish the importance of complying with AML Rules and Regulations.

Potential investors or limited partners will include qualified US institutions and accredited individuals.

COMMITMENT STATEMENT

CRESTA WESTHALL LLP IS STRONGLY COMMITTED TO COOPERATING WITH ALL APPLICABLE RULES AND REGULATIONS DESIGNED TO COMBAT MONEY LAUNDERING ACTIVITY, INCLUDING THOSE RULES AND REGULATIONS REQUIRING REPORTING OF TRANSACTIONS INVOLVING CURRENCY, CERTAIN MONETARY INSTRUMENTS AND SUSPICIOUS ACTIVITY.

IT IS THE RESPONSIBILITY OF EVERY EMPLOYEE OF CRESTA WESTHALL LLP TO MAKE EFFORTS TO PROTECT THE FIRM FROM EXPLOITATION BY MONEY LAUNDERERS. EVERY EMPLOYEE IS REQUIRED TO COMPLY WITH THE APPLICABLE LAWS AND FIRM POLICIES IN THIS REGARD. PROVEN ASSOCIATION WITH OR WILLFUL

ENABLING OF MONEY LAUNDERING ACTIVITY WILL RESULT IN SIGNIFICANT CRIMINAL, CIVIL AND DISCIPLINARY PENALTIES.

Each employee of Cresta Westhall LLP, by virtue of his or her employment by the Company, agrees to accept and abide by this Commitment Statement.

The outside brokerage accounts of the Company's associated persons will be reviewed in accordance with the procedures described in Cresta Westhall LLP's WSP Manual.

DESIGNATED PERSONNEL

The **Designated AML Program Supervisor**, or "AML Supervisor" (see table above), has been designated to implement and monitor the Company's Anti-Money Laundering Program. This individual will review any account or other activity deemed to warrant further investigation. He will act as contact point for all employees and associated persons who have suspicions or concerns—all personnel should know that they are permitted and encouraged to consult the AML Supervisor for guidance. He will act as the initial point of authority in the process of determining whether or not certain unusual activities constitute reportable suspicious activities. The AML Supervisor is also responsible for ensuring that the Company's program reflects current rules and regulations and will monitor changes to the USA Patriot Act and the Sections thereunder to ensure that policies and procedures are put into place when required. In particular, the AML Supervisor shall review changes to Section 311 to ensure that the Company implements special monitoring or supervision procedures with regard to specially designated organizations or regions.

In addition to the efforts of the AML Supervisor, certain other Company personnel will serve to implement supervision under the Company's AML Program. The **Chief Compliance Officer** will act as the central point of contact for communicating with the regulatory agencies regarding money laundering issues, unless such authority is delegated to the AML Supervisor. The CCO will act as the final point of authority in the process of determining whether or not certain unusual activities constitute reportable suspicious activities. He will also ensure that the requirements under FINRA Consolidated Rule 3310 and any new, relevant rules and regulations are implemented on a continuing basis.

The following individuals have been designated to perform various duties relating to the Company's AML program:

Area of Responsibility	**Name of Designated Party**
314(a) FinCEN reviews	Richard Pound
OFAC Reviews – Initial	Richard Pound
OFAC Reviews – Annual	Richard Pound
CIP Verification – Reviewer	Richard Pound
Review and update Firm Contacts	Richard Pound
Ongoing monitoring of activities	Richard Pound
AML Training	Richard Pound
Independent Testing	Qualified external party

Procedures relating to these duties are outlined throughout the manual and will be supervised by the AML Supervisor, unless otherwise noted.

So that the Company can promptly receive alerts from FinCEN and other entities, the Company will provide the following information to FINRA (in accordance with

FINRA's required filing format) on each associated person designated to implement the AML Program (i.e., the AML Supervisor and other individuals specifically designated to receive AML-related communications):

- Name of AML contact person,
- Title,
- Mailing address,
- E-mail address,
- Telephone number, and

Within 17 business days after the end of each calendar year, the Web CRD Administrator or appointed staff member will review and update, if necessary, the AML compliance person information. If the AML supervisor changes during the year, the Company must update the contact information promptly to ensure that notices from FinCEN are received in a timely manner by the appropriate party.

Details of the processes by which unusual or suspicious accounts and activities are handled are described below.

PRELIMINARY RISK ASSESSMENT

Cresta Westhall LLP has been formed for the purpose of assisting managers of private investment fund raise capital; beyond that, the Company conducts no securities transactions, and therefore, has no "accounts." (The terms "customer" and "account" are used in this written program because FINRA and federal regulators may apply those terms to the Company's clients and PP investors. Both "investor" and "client" are also used to describe the Company's "accounts" and "customers.") In conducting its business, the Company is committed to the "Know Your Customer" principle, reiterated below, and will complete a risk assessment for each investor purchasing securities and for each advisory client. The purpose of this risk assessment is to determine, given the types of products or transactions in which the Company operates, the likelihood of suspicious or potentially illegal activity. Registered Representatives and their designated Principals are required to consider the following factors when establishing new relationships with clients or when reviewing the activities of existing clients:

1) Whether the client is an individual, an intermediary, public, private, domestic or foreign corporation, a financial or non-financial institution, or regulated person or entity;
2) Whether the client has been an existing client for a significant period of time;
3) How the client became a customer of the Company;
4) Whether the business of the client, or the particular type of account, is the type more likely to be involved in illicit activity (e.g., cash intensive business);
5) Whether the client's home country is a member of the Financial Action Task Force (FATF) or is otherwise subject to adequate anti-money laundering controls in its home jurisdiction; and
6) Whether the client resides in, is incorporated in or operates from a jurisdiction with bank secrecy laws, or one that has otherwise been identified as an area worthy of enhanced scrutiny.

Registered Representatives are required to evaluate the risk of each new customer and if risk is perceived, bring such concerns to the attention of the AML Supervisor.

The AML Supervisor shall evaluate the facts prior to the person or entity becoming a customer of the Company and will put into place a special monitoring procedures, if necessary based on the risk. These special monitoring procedures will be outlined in the customer file and documented during reviews of applicable activities.

The RR and designated Principal should then continue to gain familiarity with the client by gathering all information in accordance with the Company's internal procedures. The risk assessment will be deemed either valid or unsubstantiated, based on the client documentation and approval process, and may be useful in the future monitoring of new client relationships, if approved.

CUSTOMER IDENTIFICATION PROGRAM

Cresta Westhall LLP endeavors to accept or solicit only those investors and clients whose source of wealth and funds can be reasonably established to be legitimate. The Company will take reasonable measures to establish the identity of its clients and will only accept them when this process has been completed.

This Anti-Money Laundering Compliance Program does not reiterate, but rather, incorporates by reference Cresta Westhall LLP's various procedures related to "Know Your Customer" and suitability standards, new account approval, existing account information updating, and applicable FINRA and SEC rules and regulations such as Conduct Rule 3110. The Company's Written Supervisory Procedures currently describe in detail its policies and procedures designed to meet regulatory requirements and ensure a high degree of familiarity with its clients. Registered Representatives are encouraged to review these procedures to ensure their comprehension and compliance.

The Company's Customer Identification Program, or CIP, is designed to meet the requirements under Section 326 of the USA PATRIOT Act. Also integrated in this section are procedures applying necessary scrutiny and information-gathering standards mandated by various other sections of the USA PATRIOT Act.

Definitions. In the context of this CIP, **"customer"** (or "client" as used herein) refers to a person who opens a new account or an individual who opens a new account for an individual who lacks legal capacity or for an entity that is not a legal person.

The following persons are excluded from the definition of "customer:"

- Persons completing new account documentation for another person, who are not also party to the account;,
- Persons with trading authority over accounts (unless necessary to verify the customer's identity): or
- Existing customers, provided the Company has a reasonable belief that it knows the true identity of such person.

The following entities are also excluded from the definition of "customer" for CIP purposes:

- a financial institution regulated by a federal functional regulator, such as
  - the Board of Governors of the Federal Reserve;
  - Federal Deposit Insurance Corporation;
  - National Credit Union Administration;
  - Office of the Comptroller of the Currency;

    - Office of Thrift Supervision;
    - Securities and Exchange Commission; or
    - Commodity Futures Trading Commission) or a bank regulated by a state bank regulator;
- a department or agency of
    - the United States,
    - any State, or
    - any political subdivision of any State;
- any domestic entity, other than a bank, whose common stock or analogous equity interests are listed on the NYSE Euronext or, AMEX, the separate "NASDAQ Small-Cap Issues" (now known as NASDAQ Capital Markets) heading.

Registered Representatives, if confused about whether or not a new customer falls under the definition of "customer" for CIP purposes, must consult their designated Principals and/or AML Supervisor for clarification.

For the purposes of CIP, an **"account"** refers to a formal relationship with the Company established to effect transactions in securities, including, but not limited to, the purchase or sale of securities.

The Company does business with entities excluded from the definition of "customer" for CIP purposes, as outlined and verified through information gathered regarding these entities, in addition to entities not excluded from the definition of "customer." For entities excluded from the definition of "customer," the Company is not required to verify the identity of these entities or their owners. The Company's procedures relative to entities not excluded from this definition are included in the rest of this section.

This section, while devoted to procedures at the opening stage of an engagement/offering, serves as a reminder to Registered Representatives to attain the highest level of familiarity possible with all customers, not only new customers. It is imperative that existing customers are also scrutinized in light of the new legislation and regulations related to money laundering. At a minimum, in keeping with revised SEC books and records rules, the Company requires that customer records be reviewed periodically to ensure up-to-date contact information and suitability data (RRs should reference their WSP Manuals for related details).

No exemptions from CIP requirements currently exist for private placement and hedge fund offerors: identification and verification must take place for customers, as defined.

Necessary Account Information

As part of its CIP standards, the Company requires its Representatives, prior to deal closing, to obtain the following **minimum identifying information** for each new investor or client, whether a person, entity or organization whose name is on the account:

- Name of the entity;
- An address, which will be a principal place of business, local office, or other physical location;

- An identification number, which will be a US taxpayer ID number, if applicable.

If a customer has applied for, but has not received, a taxpayer ID number, Registered Representatives are permitted to enter into an engagement; however, the RR must

- make note of the missing identification number in the customer file;
- obtain evidence that such an application has been made;
- record the date estimated by the customer of the pending receipt of such number;
- make efforts to obtain the ID number by contacting the customer on or about the estimated receipt date and frequently thereafter, if necessary; and
- Record all attempts to receive the number in the customer file.

Without seemingly authentic reasons for the delay, should the Company not receive the ID number within 60 days after the estimated receipt date, either the relationship must be terminated or the offeror must be notified about the inability to obtain such from the potential buyer/investor. The AML Supervisor or CCO may extend this deadline if they deem appropriate. If the Registered Representative cannot verify that an application for a taxpayer ID number has been filed or the customer has not filed such an application, the AML Supervisor must be notified to determine is further action or reporting may be required.

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the account will not be opened and the AML Supervisor will be notified. After reviewing the facts and circumstances, the AML Supervisor will determine if an existing account, if applicable, should be closed and whether the Company should report the situation to FinCEN on a SAR-SF. Notes regarding this review and recommendation will be maintained in the Company's AML files. If a filing is required, the AML Supervisor shall follow the Company's procedures related to SAR filings as included in this Manual.

Certain other information, as described below and according to customer type, must be gathered, when possible, in order to firmly establish the customer's identity and source of funds. *The Company's approach to supplemental information gathering is risk-based:* information gathered will vary according to the risks posed by the type of account. Some of the information described below may not be necessary in cases where a customer's identity is not questioned; however, in other cases, supplemental information may be required to contribute to the Company's reasonable belief that it knows the true identity of its customers. In some cases, certain information is *required* to meet federal regulations, for instance, in the case of private banking accounts and correspondent accounts for foreign financial institutions. In the event RRs are uncertain as to the extent of information required to verify the identity of any given customer, they should immediately contact their designated Principals or the AML Supervisor for guidance prior to opening the account.

Verifying documentation of all the following efforts must be maintained in accordance with the Company's established procedures, as well as those described later in this section. In addition, throughout the information gathering-process, RRs and designated Principals should make notes about their questions, concerns or suspicions, and include those notes in the respective account files.

Accounts for an Individual Living in the US— Not applicable—the Company does not accept these types of accounts. All Company employees and registered persons must report to the AML Supervisor any perceived attempt on behalf of a customer to open such an account with the Company. Should such an attempt be detected, the AML Supervisor will investigate and follow up with actions designed to halt the activities and fulfill any and all reporting obligations.

Domestic Operating or Commercial Entities—The Registered Representative should be confident about the identity of the corporate or business entity and the authority of its representative to act on its behalf. If doubt exists or risk is perceived, the RR must obtain information sufficient to ascertain the identity and authority. New customers that are LLCs should undergo scrutiny to assess the correlation between their business activities and their formation documents (i.e., description of business activities). Should the LLC be deemed a shell, further investigations into the entity's ownership (source of funds) must be conducted to determine the risk profile of the customer.

Domestic Trusts—For trust accounts, the Registered Representative must obtain information in order to verify the identity of the named accountholder (not the underlying beneficial owners) and the authorized activity of the trust.

Institutions, Hedge Funds, Investment Funds and Other Intermediary Relationships—While institutions may not represent a credit risk to the Company, they may enable money launderers, and therefore represent risk in another form. For this reason, it is imperative that scrutiny be applied to some institutions. The Company's existing procedures related to suitability and customer documentation must be followed. Being aware and assured of this information will contribute to the Company's familiarity and comfort with the customer. In order to determine whether or not further due diligence is necessary when engaging in business with a new institutional customer or continuing to do business with one, the Registered Representatives and their designated Principals or the respective fund's administrator will evaluate the following considerations:

- The institution or intermediary has authority to act on behalf of the underlying client (this can be achieved by receiving written representation of this authority);
- When appropriate, the institutional client/intermediary has policies and procedures to know its customers;
- The institution/intermediary has established anti-money laundering policies and procedures;
- The Company has historical experience with the institution/intermediary;
- The institution/intermediary is a registered financial institution based in a major regulated financial center or is a registered financial institution located in a Financial Action Task Force (FATF) jurisdiction;
- The institution/intermediary has a reputable history in the investment business; and/or
- The institution/intermediary is from a jurisdiction characterized as an offshore banking or secrecy haven or is designated as a non-

cooperative country by credible international organizations or multilateral expert groups.

If the institution/intermediary represents a new relationship, in accordance with the risk-based nature of this AML program, the RR may wish to receive written acknowledgement or confirmation of some of the topics above. Registered Representatives should be aware that institutions are not exempt from risk assessment and due diligence requirements. While risk may be more difficult to determine and information may be harder to examine, these prescribed efforts must be made. The designated Principal, in his or her reviews of new accounts and customer account activity, will look for evidence of compliance with these procedures and may compel the RR to request and receive written attestations from clients, if deemed necessary.

The Company does not do business with foreign persons or entities, private bank accounts, foreign political officials or correspondent accounts of foreign financial institutions. If the RR or designated Principal determines that one of the accounts or entities has attempted to conduct business with the Company, the designated Principal is required to take steps necessary to close the engagement and notify applicable authorities, if necessary. Should the .Company change its business to engage with such customer, the AML Supervisor shall ensure that appropriate procedures are in place prior to conducting business with such customer.

C. Verification of Identity The Company's goal is to know, based on a reasonable belief, the true identity of its clients. Toward that goal, Registered Representatives are required to attempt to verify each client's identity and document such verification efforts. During this process, RR's and other Company personnel are expected to note and analyze any logical inconsistencies in the information obtained.

Documentary Means. Documentary means of identification will not ordinarily be used. In certain cases, RR's and/or the respective fund's administrator may attempt to verify investors' and clients' identities through documentary means. Possible sources of information include:

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

The Company is not required to maintain copies of the documents reviewed during the verification process but must record information related to the document sufficient to evidence their review. This information must include the type of document reviewed, the issuer of the document (i.e. state or country). In the case of a picture id, such as a driver license or passport, the identification number and the expiration date should also be recorded. In the case of corporate documents or business license, a file number or license number and date of issuance should be recorded. The AML Supervisor or his designee shall verify that adequate information has been recorded in the Company's files during his reviews and shall evidence his review by initialing and dating the applicable documents in the customer file.

RR's are not expected to determine whether such documents are valid; however, if some obvious form of fraud is evident, RR's should not accept the document as verification and should consult the AML Supervisor for assistance and to attempt to verify identity through other means (such as non-documentary methods).

Non-Documentary Means. In most cases, non-documentary methods of verification will be necessary—either alone or in combination with documentary means. RR's must use non-documentary methods (outlined below) in the following situations: (1) when the investor or client is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard; (2) when the Company is unfamiliar with the documents the investor or client presents for identification verification; (3) when the investor or client and Company do not have face-to-face contact; and (4) when there are other circumstances that increase the risk that the Company will be unable to verify the true identity of the investor or client through documentary means.

Non-documentary methods of verifying identity include:

- Contacting the investor or client at his residence or place of business;
- Independently verifying the investor's or client's identity through the comparison of information provided by the investor or client with information obtained from a consumer reporting agency, public database, or other source;
- Checking references with other financial institutions;
- Obtaining a financial statement; and/or
- Any other reasonable means of attempting to verify the investor's or client's identity, such as testing phone numbers or e-mail addresses provided.

In cases where non-documentary verification is used, the Company must retain a copy of the information gathered during this review as evidence of their verification efforts. The documentation may include notes regarding contacts with the customer or references, copies of financial statements or reports from consumer reporting agencies. Where a web search is used to verify identity or information provided by the customer, the Company should utilize information from a source other than one created by the customer in its verification efforts and should maintain a copy of the web pages reviewed as evidence of verification. The AML Supervisor or his designee shall verify that adequate information has been retained in the Company's files during his reviews and shall evidence their review by initialing and dating the applicable documents in the customer file.

Timing. Registered Representatives must attempt to verify the identities of new customers. During face-to-face meetings, ID documents should be viewed and noted. If the RR does not receive sufficient information to verify the identity of a new customer the following procedures must be followed:

- If a potential customer is known to the firm or its principals because of a prior relationship or the manner in which he or she was introduced to the firm, such as a referral from an existing customer, the representative should contact the AML Supervisor prior to entering into a relationship/engagement with the customer, so the Supervisor may make a determination on the potential risk based on the type of business to be conducted and other information known about the customer. The AML Supervisor shall document his/her review and shall advise the registered representative whether or not the engagement may be entered into, prior to verification.

The AML Supervisor's decision and any restrictions on the relationship shall be noted in the client file.

- If a potential customer is completely unknown to the Company and the RR, or could be construed to represent higher risk (based on the specific customer profile), verification of identity must take place before the deal is closed. Reluctance on behalf of the potential customer may be considered suspicious and should be brought to the attention of the AML Supervisor so that he/she may determine whether additional action is required. Documentation related to the customer and the AML Supervisor's determination shall be maintained by the AML Supervisor in his potential suspicious activities file.

The Company is not required to verify the identities of individuals with authority or control over activities of the customer (of non-individuals, for example) on which they are not named as parties to the transaction. However, in the event insufficient verification is available to identify such customers, RR's must attempt to obtain information on the individuals with authority or control over these customers. Failed attempts are valid reasons for not entering into an engagement or relationship.

In all cases, if efforts to verify the identity of the customer fail, the RR should consult the AML Supervisor to determine further action. If deemed necessary a Preliminary Suspicious Activity Report should be completed and reviewed by the CCO. See "Reporting Procedures—Internal," below.

D. Comparison with Government Lists In reviewing existing accounts or obtaining information in order to open new accounts, Registered Representatives should, given the profile of the accounts as determined above, consult certain lists in order to determine if such accounts are "blocked" or subject to certain controls.

Office of Foreign Assets Control (OFAC). In Notices 97-4, 97-35, and 02-21 FINRA reminds all member firms about the Department of the Treasury rules issued by the Office of Foreign Assets Control (OFAC). OFAC rules do not fall under the USA Patriot Act. These rules are separate and enforceable by the Office of Foreign Assets Control. Under these regulations and a 2001 Executive Order targeting terrorists, the Company cannot deal with certain individuals or in securities issued from certain identified target countries.

The Company must block or freeze assets and obligations of blocked entities and individuals when their property is in their possession or control (or, in certain cases, transactions must be rejected). "Blocking" is a legally enforceable freeze on the utilization of any account or asset without authorization from OFAC. The Company is prohibited from engaging in transactions for blocked entities or individuals. Blocked SEC securities may not be paid, withdrawn, transferred (even by book transfer), endorsed, guaranteed or otherwise dealt in. The following are examples of designated entities under the 2001 Executive Order:

- Usama Bin Laden
- Abu Sayyaf Group
- Al-Hamati Sweets Bakeries
- Al-Barakaat
- Abu Bakr Ahmad
- Al-Aqsa Islamic Bank
- Parka Trading Company

- Continuity IRA
- Certain North Korean entities designated "proliferators WMD"

Examples of entities or nations subject to OFAC sanctions and requiring blocking include the following (not all are listed here):

- Specially Designated Nationals and Blocked Persons (SDN's) (including terrorists, narcotics traffickers, foreign terrorist organizations and kingpins),
- Cuban citizens unless US residents,
- Individuals or entities in Cuba;
- Certain persons or entities in Burma, Balkans, Iran, Liberia, North Korea, Syria and others;
- Governmental entities and officials of Cuba and Sudan.

The Office of Foreign Assets Control ("OFAC") lists must be reviewed for all new customers and the Company must screen their existing customers against these lists at least annually. OFAC Specially Designated Nationals and Blocked Persons (SDN) lists can be reviewed by on the OFAC website, www.ustreas.gov/ofac, or by using the OFAC search at http://apps.finra.org/rulesregulation/ofac/1/Default.aspx). The Company will retain evidence of the initial review in the client file. Evidence of annual reviews may be retained in either the client file or a separate OFAC review file.

If the Company is doing business with non-public entities, that are not federally regulated, where the owners or principals are unknown to the Company or would normally be subjected to additional scrutiny, such as foreign individuals or entities, the Company must screen the owners or principals against OFAC prior to opening an account or entering into a relationship and at least annually thereafter. Evidence of this review must be maintained in the client or OFAC review file.

RRs with concerns about specific existing customers are encouraged to search these sites directly in an effort to expedite and enhance Company anti-money laundering efforts.

The Company may register with OFAC's e-mail subscription services to receive information and updates. By being familiar with OFAC's website, the Company will enhance its ability to promptly detect possible customer matches, thereby avoiding penalties for non-compliance. The Company must maintain some evidence of its efforts to check OFAC lists (for instance, a log or an electronic record of searches).

During a search, if a match is found, internal due diligence must take place to determine that a number of similarities exist BEFORE calling the OFAC hotline. (In other words, the Company must attempt to confirm that the match is a "true hit" and not a "false positive.") Similarities include such items as:

- Person versus organization
- Same complete name spelling
- Same first and last name (not just last name)
- Same country location
- Same address, if known
- Same or similar aliases, or former names
- Same nationality, and
- Same date of birth or close age

If a search results in the customer's country being identified as under "limited" sanctions, the Company may continue without reporting to OFAC. In cases where questions remain after attempting to rule out a false positive, the Company should contact OFAC for assistance.

If a match is confirmed, the CCO must inform OFAC, within 10 days, on its hotline (1-800-540-6322) and must inform the customer and other appropriate parties that the assets or accounts are blocked. The CCO should review the securities in the Company's custody (if applicable) to determine whether those that are blocked under current sanctions are properly treated. These include debt and equity securities representing SDN governments and companies. The CCO should then scrutinize any other securities that could reasonably represent obligations of, or ownership interests in, entities owned or controlled by blocked commercial or governmental entities. All required forms, such as the blocked assets form and rejected transaction form, must then be filed, as directed and supervised by the CCO.

Lack of compliance with OFAC rules may result in civil or criminal penalties.

Other Lists. The Company may, from time to time, receive notice that a federal government agency has issued a list of known or suspected terrorists. Within a reasonable period of time, after an engagement or relationship is opened (or earlier, if required by another federal law or regulation or federal directive issued in connection with an applicable list), the AML Supervisor will 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 the Department of the Treasury in consultation with the federal functional regulators. The AML Supervisor will ensure that the Company follows all federal directives issued in connection with such lists. NOTE: the Company must not contact OFAC if it discovers a match to a non-OFAC list. Only matches to names on OFAC lists should be reported to OFAC.

Further, the AML Supervisor shall monitor enhanced or new requirements as implemented under Section 311 regarding specified organizations or regions and shall develop and implement procedures to address such requirements. Because these requirements are generally temporary in nature, changes in the Company's procedures will generally be communicated through inter-office communications, rather than through a change to the procedures manual. Should any requirements under Section 311 become permanent with respect to specific organizations or regions, then the Company shall evaluate its procedures to determine if permanent changes are required.

E. Additional Due Diligence As mentioned above there may be instances where more information is required in order for the Company to meet its CIP obligations. Following the Company's efforts to authenticate its clients' identities, questions may remain. These questions should be brought by the RR or his/her designated Principal to the AML Supervisor, who may decide to make use of the following to assist in verifying and/or providing customer information:

- Business database searches,
- Media searches,
- Investigations by outside consultants,
- Contacts with international enforcement agencies (such as Interpol), and
- Reviews of all relevant lists (see below).

The purpose of such additional due diligence may be to explain discrepancies in a customer's SSN or TIN, date of birth, residential address, etc.

Another reason for conducting further research would be if the RR or designated Principal suspected a client to be located or incorporated in certain countries or regions identified by recognized international organizations, multilateral expert groups or in governments or industry publications as noncooperative with international anti-money laundering principles or procedures or having inadequate anti-money laundering measures. To follow are some of the sources the AML Supervisor may consult in order to categorize the account as high-risk or a member of a non-cooperative jurisdiction:

- The Financial Action Network Task Force on Money Laundering ("FATF"),
- Patriot Act Section 311 Designated Countries,
- U.S. Immigration and Naturalization Service (INS),
- The Financial Crime Enforcement Network ("FinCEN"),
- The Organization for Economic Cooperation and Development ("OECD") and
- The U.S. Dept. of State's annual International Narcotics Control Strategy Report ("INCSR") and CIA Fact Book.

In the event additional due diligence is conducted, the designated Supervisor must ensure that all information received will be kept in the client's account file, and will remain confidential. This information, if indicative of suspicious activity, will be used in internal or official reporting, described below.

For specific enhanced due diligence and scrutiny that must be applied to Private Banking Accounts for non-U.S. persons, including Senior Foreign Political Figures, and Correspondent Accounts for certain foreign financial institutions, see the text above under "Necessary Account Information."

The Company, in applying any such additional measures, will comply with all privacy requirements.

F. Suspicious Activity—Account/Relationship Opening Stage Registered Representatives and their designated Principals, in the process of gathering customer information and researching the subjects addressed above, must remain alert and aware of their prospective clients' actions and attitudes throughout the process. While suspicious activity may normally occur in the course of servicing existing clients, certain actions by a prospective client during the account opening stage may be indicators of money laundering intentions. By being perceptive, Registered Representatives will have the opportunity to take note of such indicators, which may include:

- Verification of a client's identity proves unusually difficult and/or such client is reluctant to provide full details with respect to his or her identity, type of business and assets, and business activities, or furnishes unusual or suspect identification or business documents;
- A client who wishes to engage in transactions that lack business sense, apparent investment strategy, or are inconsistent with the client's stated business and/or strategy;

- A client whose requirements are not in the normal pattern of or inconsistent with the Company's business which could be more easily serviced elsewhere;
- A client, or person publicly associated with the client, has a questionable background or is the subject of news reports indicating possible criminal, civil or regulatory violations;
- Difficulties and delays in obtaining copies of documentation related to incorporation or authorization;
- The address of an LLC is found to be listed as the address of several LLC's;
- The client's (if an entity) business activity apparently conflicts with the description of activity listed on its formation documents;
- An institutional or intermediary client demonstrates ignorance of expectations regarding AML regulations and/or unreasonable denial of requests for assurances relating to its own internal customer acceptance and/or AML policies and procedures;
- A client appears to be acting as the agent for another entity but declines, evades or is reluctant, without legitimate reasons, to provide any information in response to questions about that entity.

Any such behavior noted in the account opening or reviewing stage must be noted in writing by the observer and maintained in the client's file. These observations, if determined valid, will used in internal or official reporting, described below.

G. Records/Retention The Company must maintain a record of all identification information for five years after the account is closed; records made about verification must be maintained for five years after the records are made.

H. Reliance on Another Financial Institution The SEC has granted a limited exemption so that firms may rely on another financial institution to perform some or all of the functions required to identify customers. OFAC rules generally do not recognize the ability of firms required to conduct OFAC screenings to rely on another person or entity to conduct these screenings on their behalf. Firms entering into agreements with outside entities, including their clearing firm, to perform OFAC checks should verify that the screenings are being conducted and are accurate as they may still be held liable for any discrepancies or missed findings.

I. Resolution The net result of compliance with the requirements described and referenced in this section is a solid familiarity with the Company's new and existing accounts. Should the information gathered under this process result in suspicions of money laundering involvement, certain actions must be taken, depending on the nature and source of the suspicions. For instance, internal reporting and/or further monitoring of the account may be conducted to assess the validity of the suspicion; or immediate official reporting may be necessary if the suspicions are judged solid. The following sections describe these choices in further detail.

MONITORING TRANSACTIONAL ACTIVITY

Besides striving to "know your customer," an objective of Cresta Westhall LLP's anti-money laundering efforts is to identify potentially suspicious and unusual activity in its clients' accounts. Monitoring transactions is essential to determining if unusual or suspicious activities are taking place, which may be related to money laundering.

A. Ongoing Monitoring Cresta Westhall LLP is currently in the practice of monitoring its business activity by conducting reviews on an ongoing basis . Such reviews may be either manual or automated. These procedures are described in the Company's Written Supervisory Procedures Manual, and comprise an important part of RR and account supervision. While these reviews were designed specifically to meet FINRA and other regulatory requirements, their implementation is useful in identifying money laundering or illegal activity. This Anti-Money Laundering Compliance Program incorporates by reference the existing transaction, trade and RR supervisory reviews and approval processes currently in use by the Company.

All Registered Representatives, back office personnel and their designated Principals, in conducting business with customers, processing business and in reviewing/approving such business, must make an attempt to identify unusual or suspicious activity. Because suspicious activity can occur long after an account has been opened and a relationship has been formed between broker and client, all transactions should be viewed in the context of other account activity and whether or not a transaction is considered suspicious will depend on the customer and the particular transaction, compared with the customer's normal business activity. Transactions that lack a reasonable economic basis or recognizable strategy, in the context of the customer's historical activity, may be a "red flag" and warrant closer inspection.

B. Suspicious Activity—Possible Red Flags While there is no definition of "unusual or suspicious," certain indicators may evidence money laundering activity. The Company's clients generally do not engage in 'transactions' other than, for instance, the closing of private placement investment. Examples of certain indicators worth noting and following up on are to follow; while some of these may not seem applicable, they are included here to remind personnel to investigate if clients attempted such actions:

- A customer provides unusual or suspicious identification documents that cannot be readily verified.
- A customer is reluctant to provide complete information about nature and purpose of business, prior banking relationships, anticipated account activity, officers and directors or business location.
- A customer refuses to identify a legitimate source for funds or information is false, misleading or substantially incorrect.
- The customer's background is questionable or differs from expectations based on business activities.
- A customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents or asks for exemptions to the Company's policies relating to the deposit of cash and cash equivalents;
- A customer attempts to engage in, transactions involving cash over $10,000 or cash equivalents or other monetary instruments that appear to be structures to avoid government reporting requirements, especially if the monetary instruments are in an amount just below reporting thresholds and/or are sequentially numbered;
- A customer wishes to engage in multiple transfers of funds or wire transfers to and from countries that are considered bank secrecy or "tax havens" that have no apparent business purpose or are to or from countries listed as non-cooperative by FATF and FinCEN (see "Additional Due Diligence" above), or are otherwise considered by Cresta Westhall LLP to be high-risk;

- A customer attempts to make a funds deposit knowing the Company does not accept them;
- A customer purchasing a long-term investment, followed shortly thereafter by a request to liquidate the position;
- For no apparent reason, a customer has multiple investments or business under a single name or multiple names;
- A customer requests that a transaction be processed in such a manner so as to avoid the Company's normal documentation requirements; and
- A customer exhibits a total lack of concern regarding risks, commissions, or other transaction costs

Registered Representatives, back office personnel and their supervisors must be familiar with these indicators and must make note of them, if perceived, in the client's file. Notes to this effect will be used in determining if reporting is necessary, as described later in this Program.

C. Specific Activity Monitoring Certain account activity may be more indicative of money laundering practices than others. Cresta Westhall LLP has adopted the following procedures in order to facilitate its detection of such illicit practices:

1) **Wire Transfers**. The Company does not perform or coordinate wire transfers for its clients.

   Should the Company ever make wire transfers, it will confirm that proper record keeping under the "Travel Rule" is conducted. The "Travel Rule" arises under the Treasury Department regulations issued by the FinCEN pursuant to the 1996 amendments to the BSA. Should the Company transmit funds equal to or greater than US$3,000 (or its foreign equivalent), it will include in its transmittal order the following records, to be maintained for a period of five (5) years:
   - Name, address and account number of transmitter;
   - Identity of transmitter's financial institution;
   - Amount of the transmittal order;
   - Execution date of order;
   - Identity of the recipient's financial institution; and,
   - If received, the name, address and account number of recipient and any other specific identifier.

2) **Cash Receipts**. The Company does not accept cash or carry customer accounts. Should a customer attempt to make a cash deposit, the attempt should be rejected, notes of the attempt should be kept and the AML Supervisor should be notified.

3) **Cash Equivalents**. The Company does not accept cash or cash equivalents, including cashier's checks, money orders and traveler's checks. Should the Company receive any such instruments, it must log the receipt on its Checks Received and Disbursed log before returning the instruments with instructions on proper funds remittal. Should the Company receive a check made payable to a private placement issuer, it will log such check on its Checks Received and Disbursed log prior to forwarding the check to the payee. The AML Supervisor will review this log monthly in order detect potential structuring of such deposits.

4) **Foreign Currency Transactions and Foreign Accounts.** The Company does not accept any cash payments in foreign currency or from foreign transactions for securities purchases. Should a customer attempt to make such a payment, the attempt should be rejected, notes of the attempt should be kept and the AML Supervisor should be notified.

5) **High Risk Customers.** As a result of the Company's compliance with these anti-money laundering procedures, certain customers may be targeted as "high risk" or "red-flagged." All such customers will have been brought to the attention of the designated Principals and AML Supervisor according to the policies described below under "Reporting." The designated Principal supervising the RR serving such customers will have the responsibility to monitor more closely all activity of these customers. In addition, the AML Supervisor, monthly, will consult this list of customers and consult with either, or both, the respective RR and designated Principal as to recent customer activity. The AML Supervisor will record notes on these consultations in the customer's file.

6) **Exceptions.** The Company does not make use of exception reports.

Results of the monitoring described here may require inquiry or investigation on behalf of the AML Supervisor in an effort to gain reasonable explanations, given the respective client's profile, or to justify suspicion. Any resulting reporting will be conducted as described below.

The AML Supervisor may decide that fulfillment of these monitoring responsibilities must be supported through the use of automated or other means. In this event, new policies will be implemented and added to this Program to describe such monitoring.

REPORTING PROCESS

The procedures described above--preliminary risk assessment, "know your customer" practices and transaction monitoring—are intended to promote the detection and deterrence of money laundering and other illegal activities. Compliance with these procedures may lead to concerns about unusual activity or clear suspicions related to a customer's behavior or intentions. To follow are the steps Company personnel should take in order to resolve these concerns.

A. Definite Suspicious Activity In the event any Registered Representative, operations ("back office") personnel, designated Principal or other employee of the Company has clear evidence of suspicious activity, s/he must immediately report such to his or her designated Principal (Principals must report directly to the AML Supervisor). Such activity may consist of a customer being listed on OFAC or SEC Control Lists, as described above, or a customer exhibiting a blatant indicator of suspicious activity, as described above. Definite suspicious activity may be detected in any of the stages described in this Program: preliminary risk assessment, "know your customer" practices and transaction monitoring.

Once such activity is detected, the employee should consult his or her supervisor and discuss the suspicion. The designated Principal's involvement will serve as an initial "sanity check" of the reported activity. At this stage, if the designated Principal can confidently dispel the suspicion, notes on the dismissed event should

be included in the customer's file, for future reference, if necessary. Should the suspicion appear valid, the employee and designated Principal together must complete a Preliminary Suspicious Activity Report (see "Forms"), described below under "Reporting Procedures—Internal," and immediately report to the AML Supervisor.

In certain situations, the AML Supervisor or Chief Compliance Officer should immediately contact Federal law enforcement by telephone. Example of such emergency situations include:

- A client is listed on the OFAC list;
- A client's legal or beneficial account owner is listed on the OFAC list;
- A client attempts to use bribery, coercion, undue influence, or other inappropriate means to induce the Company to open an account or to proceed with a suspicious or unlawful activity or transaction; and
- Any other situation the Company has determined to require immediate governmental intervention.

The Company, if it files a blocking or other report with OFAC on one of its clients, is not required to also file an SAR-SF with FinCEN. OFAC will report filed information to FinCEN. However, if suspicions exist beyond the details provided in the field OFAC report, the Company must file a separate SAR-SF with FinCEN to report those suspicions.

B. Supposed Unusual or Suspicious Activity In following the procedures outlined above, including preliminary risk assessment, "know your customer" practices and transaction monitoring, a RR or other employee may come to suspect an account of engaging in unusual activity that could feasibly be linked to money laundering. The employee may base his or her suspicions on any of the guidelines provided above—for instance, an existing account suddenly and inexplicably changes his investment strategy and deals in multiple dollar amounts below reporting thresholds. Or, for instance, a Registered Representative, having completed the preliminary risk assessment and conducted reviews of his or her client's account documentation in an effort to better know his/her client, has recorded certain notes in the client's file (as required above) and as a result, has heightened suspicions regarding the account's transaction activities. In cases such as these examples, where suspicions exist, yet may not appear definite, the following steps must be taken.

As with "definite suspicious activity," once suspicions exist, the employee should consult his or her supervisor and discuss them. The designated Principal again will serve to provide an initial "sanity check" of the reported activity. At this stage, if the designated Principal can confidently dispel the suspicion, notes on the dismissed event should be added to the client's file, for future reference, if necessary. Should the suspicion appear valid, the employee and designated Principal together must complete a Preliminary Suspicious Activity Report, described below under "Reporting Procedures--Internal."

Note that RR's and all employees may have suspicions at any stage of their involvement with clients. Suspicions of unusual activity should be based on sound evidence and reasoning: the employee must not rush to judgment. However, equally important is the need to communicate with supervisors. An employee should not attempt to build a complete case against a client without the review of his or her designated Principal; in other words, accumulating notes and monitoring account activity in order to gain confidence about a suspicion is advisable, but

waiting too long to report such suspicion may be ultimately detrimental to the Company.

C. Reporting Procedures—Internal The **Preliminary Suspicious Activity Report** (P-SAR) is designed to provide for an internal review prior to official reporting, in order to avoid unsubstantiated (and embarrassing) official reporting. The designated Principal must forward the completed P-SAR to the AML Supervisor for review. The AML Supervisor will review the details related to the suspicious activity and will then recommend any of the following: dismissal of the suspicion, based on his or her own knowledge of the account or activity; focused monitoring of the account in question in order to confirm or dispel suspicions; investigation of the transaction or activity by another party such as General Counsel or internal legal professionals; or immediate official reporting. If accounts or activities are determined to require further monitoring or investigation, the AML Supervisor will implement such monitoring and track the results in order to later make another decision about the suspicious activity: to dismiss or officially report.

Final resolution of all issues reported via P-SAR's is required. The AML Supervisor will record the results of his or her reviews on the "**P-SAR Review Form**," and provide a copy of this form to the CCO for final approval. The CCO may recommend an alternative course of action or give his or her consent. If immediate official reporting is warranted, the Chief Compliance Officer will conduct such reporting, as described below. Note that completed P-SAR and P-SAR Review forms must be maintained in the AML Supervisor's files, and kept confidential (not to be disclosed to the customer or any other unauthorized party).

It is necessary that the Company and its personnel be able to justify why, in the face of certain suspicions or account activity, no formal SAR reporting was conducted. Regulators insist on seeing documentation to substantiate a non- SAR filing. For this reason, it is imperative that all suspicions and supervisory follow-up are well documented (even if P-SAR and P-SAR Review Forms are not used in certain instances).

D. Reporting Procedures—Official Since 1996 broker-dealer subsidiaries of bank holding companies have been required to file a Suspicious Activity Report on suspicious transactions relating to possible money laundering activity. Many other securities firms have voluntarily filed such forms with FinCEN or contacted law enforcement directly when suspicious activity of this nature has been identified. Section 356 of the USA PATRIOT Act requires ALL broker-dealers to file **Suspicious Activity Reports by the Securities and Futures Industry** (SAR-SF or FinCEN Form 101), and FINRA Consolidated Rule 3310 mandates this reporting. The U.S. Treasury requires broker-dealers to report any questionable transaction or series of transactions in excess of $5,000; however, voluntary reporting may take place for smaller dollar amounts in question.

The CCO, once having determined to file an SAR-SF (see forms section for a sample), will complete and file the form with FinCEN within 30 days of being aware of the suspicious transaction(s). Reporting can also be done electronically through the Patriot Act Communication System at http://pacs.treas.gov/index.jsp. If the Company is an introducing broker, only one SAR-SF need be filed, either by the Company or its clearing firm. A copy of the form or confirmation page of an electronic filing and all supporting documentation must be retained for five years, and kept confidential (not to be disclosed to the customer, employees not involved in

the filing process—including the RR on the account, or any other unauthorized party).

The Company is not required to cease doing business with customers that are the subject of a filed SAR-SF. The CCO and AML Supervisor must use their discretion in these cases. If accounts are left open, the designated Principal must monitor account activity carefully, wait for a response from FinCEN or other authority and continue to file SAR reports every 90 days if the activity continues.

In some cases FinCEN or another law enforcement agency may request that the Company keep the account open so they can conduct ongoing surveillance. This request must be in writing and specify the duration of time the account is to remain open, not to exceed 6 months. If the agency wishes the account to remain open longer than six months, it must provide the Company with subsequent written requests. The Company should verify the identity of the individual and agency making the request prior to granting such a request. The Company may refuse to honor this request as ultimate responsibility for the decision to keep an account open, ongoing monitoring and ongoing SAR report filing rests with the Company and its Principals.

Company personnel seeking assistance with FinCEN forms or related issues should consult FinCEN's website at www.fincen.gov. The website provides specific guidance on BSA compliance as well as helpful information on information sharing, response to alerts and current trends in financial crimes.

Additional, related reporting may also be required of the Company, as follows (note: for specific reporting instructions, the AML Supervisor must carefully review all instructions provided on the respective reporting form):

- **Currency and Monetary Instrument Transportation Report.** Pursuant to SEC Rule 17(a)-8, it is the policy of Cresta Westhall LLP to require the designated Principal's approval prior to accepting any cash payments in foreign currency or from foreign transactions for stock purchases or amounts to be credited to the customer's account. Furthermore, any person who physically transports, mails, or ships currency or other monetary instruments into or out of the U.S., in aggregated amounts exceeding $10,000 at one time, must report the event on a Currency and Monetary Instrument Transportation Report (CMIR). Any person who receives any transport, mail, or shipment of currency, or other monetary instrument from outside the U.S. in such an amount must also report the receipt. It is the designated Principal's responsibility to ascertain that the form, U.S. Customs Form 4790, is completed and forwarded to the CCO for filing with the Commissioner of Customs. A copy must be retained in the customer's file. This form must be filed regardless of the nature (suspicious or not) of the respective transaction.
- **Currency Transaction Report.** The Bank Secrecy Act requires the Company to file currency transaction reports (CTR or FinCEN Form 104) in accordance with Treasury regulations. These regulations require the Company to file a CTR whenever a currency transaction exceeds $10,000 (whether in one lump sum or aggregating amounts). This form must be filed even if the transaction is not suspicious; if it is suspicious, an SAR-SF must be filed in addition to the CTR. A sample CTR form is attached.
- **OFAC or SEC Reporting.** Should a customer be identified as an entity listed on current OFAC lists or the SEC Control List, the CCO must

immediately contact these institutions in order to provide details and follow-up, if necessary. OFAC's Reporting, Procedures and Penalties Regulations at 31 CFR part 501 require the Company to block and file reports on accounts, payments, or transfers in which an OFAC-designated country, entity, or individual has any interest. These reports must be filed with OFAC within ten business days of the blocking of the property.

- **Foreign Bank and Financial Accounts Reports (FBAR).** Dept. of Treasury Form TD F 90-22.1 must be filed by U.S. citizens having a financial interest exceeding $10,000 in foreign accounts. The Company is not required to file such reports on behalf of its customers, but should advise its clients of their obligation to file, and should request and maintain copies of such forms. If the Company holds, or has signature authority or other authority over, a financial account in a foreign country of more than $10,000, the Company must file an FBAR with FinCEN. A sample form is attached.
- **State Reporting.** Certain states require reporting to a state authority. The CCO, upon filing official forms with federal authorities, should make efforts to determine respective obligations of the state where the Company is domiciled.

RECORD KEEPING

The Company will maintain records consistent with its established record keeping policies described in its Written Supervisory Procedure Manual. Such records include account documentation, transaction records, account and transaction review documentation and various blotters, ledgers and logs.

Records created as a result of compliance with this Anti-Money Laundering Compliance Program will include the following:

- Forms filed with federal and state authorities, such as SAR-SF, CTR, Report of International Transportation of Currency or Monetary Instruments, Report of Foreign Bank and Financial Accounts; and any other forms required, such as the "Certification for Purposes of Sections 5318(K) of Title 31, U.S. Code";
- Internal reporting documents, including the Preliminary SAR and P-SAR Review form;
- Notes, analyses and reflections of Company personnel, such as the Preliminary Risk Assessment, RR notes to account files and the results of monthly monitoring of specific activities, such as wire activity; and
- Results of independent testing for compliance with this Program (described below).

In accordance with 31CFR 103.33, the Company will create and maintain SAR-SFs, CTRs, CMIRs, FBARs, and relevant documentation on customer identity and verification and funds transfers and transmittals as well as any records related to customers listed on the OFAC list. The Company will maintain SAR-SFs and their accompanying documentation for at least five years and will keep other documents according to existing BSA and other record keeping requirements, including certain SEC rules that require six-year retention.

CONFIDENTIALITY AND DISCLOSURE/RESPONSE TO AUTHORITIES

Confidentiality. Neither the Company nor its employees may notify any person involved in a reported transaction that the transaction has been reported on an SAR-SF. The Company must also not divulge any information on a SAR filing to any employee not directly involved with the filing or to any non-parent affiliate of the Company. In general, the Company and its employees are prohibited from disclosing SAR-SF's or the fact that they were filed, other than to law enforcement agencies or securities regulators. However, information underlying the filing (not the filing itself) may be disclosed to entities affiliated with the Company or other entities with whom the firm has a relationship, such as a clearing firm, if a 314(b) notification has been file by the Company and the other entity.

The Company has no parent entities; should its ownership structure change to include one or more parent entities, the AML Supervisor will ensure that this AML Program is amended to include procedures on sharing SAR's with parent entities.

In the event the Company receives a subpoena requesting an SAR-SF or related information, the request should be forwarded immediately to the AML Supervisor. The AML Supervisor must deny the subpoena request and inform FinCEN of any subpoena received. NOTE: Privacy policies under Regulation S-P do not apply to information provided to FinCEN in an SAR-SF and the Company and its employees are protected from liability for such required disclosures.

Information Sharing. Sharing information with other entities may be necessary to ensure that all facts related to suspicious customers or activities are known. If the Company decides to share information with other financial institutions about those suspected of terrorism and money laundering for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities, the AML Supervisor will file with FinCEN an initial 314(b) certification before any sharing occurs and annually on the anniversary of the previous filing. The certification form may be found at www.fincen.gov. Once a firm has filed this certification, it can access the names of other institutions with whom it is acceptable to share information.

The Company does not share information with other entities and does not maintain a clearing relationship. Therefore, no 314(b) certification filing has been made. Should the Company wish to share information with another entity or if they enter into a clearing relationship, the AML Supervisor shall ensure that the 314(b) filing is made prior to sharing any information or once the clearing arrangement is effective.

Response to FinCEN requests. The AML Supervisor is designated to respond to all requests made by FinCEN relating to money laundering or terrorist activity. The AML Supervisor should provide all requested information (within the confines of Section 314 of the USA PATRIOT Act) to FinCEN as soon as possible, either online, by e-mail to patriot@fincen.treas.gov, by calling the Financial Institutions Hotline (1-866-556-3974) or according to FinCEN's instructions.

After receiving a "314(a)" request, or reviewing web-enabled delivery of such requests, the AML Supervisor or his designee shall review the lists against a listing of the Company's current clients and any clients with whom they have conducted business within the previous 12 months, to determine if any persons or entities

appear on the list. The review must occur within 14 days or the time period identified on the request,

If a match is found (the subject of the request is located in the Company's records and the Company has used all available information to confirm the match), within two weeks the AML Supervisor must disclose to FinCEN that it has a match. The requesting law enforcement agency will then follow-up directly with the Company. The AML Supervisor must ensure that records are maintained to evidence the Company's review of these FinCEN requests. FinCEN's system includes an option for the firm to print a report to evidence the review of the current requests.

The Company will print the self-verification report as provided in the FinCEN system to evidence the review of the FinCEN 314(a) requests. Should the Company receive requests from other enforcement authorities, the AML Supervisor must respond to such requests within seven days of receiving a written request.

Response to Authorities. Should the Company receive a written request from a federal law enforcement officer for information concerning correspondent accounts, it will provide that information to the requesting officer not later than 7 days after receipt of the request. The AML Supervisor will ensure that, within 10 days, the Company will close any account for a bank--that it learns from Treasury or the Department of Justice--has failed to comply with a summons or has contested a summons The AML Supervisor or his/her designee will scrutinize any 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 accounts.

All requests received for information on suspicious activities or for copies of documentation should be verified by the AML Supervisor or his/her designee. The designated person should verify the identity and authority of the individual and/or agency requesting the information so as to protect the confidentiality of such information.

INDEPENDENT TESTING

Frequency of Testing. The Company's AML Program will be tested every calendar year.

Purpose of Testing. Compliance with this Program will be tested periodically to determine its efficacy. In general, the purpose of the testing is to assess the adequacy of the written program and to assess the Company's degree of compliance with its AML procedures. Specific goals of the audit procedures should include the following:

- Confirm the integrity and accuracy of the procedures for the reporting of large currency transactions;
- Include a review of forms filed with authorities, such as FinCEN Forms 104 (CTR) and 101 (SAR-SF), 4790 (CMIR), etc.;
- Confirm the integrity and accuracy of the Company's record keeping activities and adherence to in-house record retention policies;
- Confirm compliance with the Company's "know your customer" policies by conducting a review of a sampling of new account documentation, account reviews and transaction reviews;

- Review the AML Supervisor's records as they relate to specific monitoring of transactions or clients, or follow-up on reported unusual activity;
- Confirm adherence to the Company's internal reporting procedures;
- Confirm that all employees have been made aware of the Program, and have signed Attestations required by the Company;
- Include steps necessary to ascertain that the Company is conducting an ongoing training program; and
- Confirm that the Company's Anti-Money Laundering Compliance Program incorporates changes required as a result of new legislation or regulation.

The reviewer may choose to convey the results of his or her review in a **Summary Report of Findings** (see attached) and/or in another detailed findings report. The AML Supervisor must present all reports to the CCO of the Company. The results of testing will alert the Company's senior management to any deficiencies in the Company's AML Program and will allow the Company to take corrective and/or disciplinary action, as each situation warrants. In general, periodic reviews and testing will be used as a basis for improving compliance with the Program. The CCO shall ensure that corrective is taken when necessary and that copies of all reports of findings are maintained for a period of no less than five years.

Appointed Testing Personnel. The Company will appoint an outside party prior to the due date of the first test. The CCO will review this party's qualifications and has determined that he or she is qualified to conduct testing as required under Consolidated FINRA Rule 3310.

EMPLOYEE TRAINING

Cresta Westhall LLP is committed to training and educating its registered representatives and other applicable persons on the identification and prevention of money laundering and other illegal activities. The Company has appointed the AML Supervisor to provide AML training to supervisory and registered personnel. Certain employees will require additional, specific training if their roles merit it (for instance, cashiering, margin or other operations personnel) and the AML Supervisor will coordinate such additional training, when necessary.

Training will be provided annually or more frequently, when deemed appropriate by the AML Supervisor, and the materials and discussions will address, at a minimum, the following:

- The Company's "know your customer" policy and procedures;
- Potential indicators of suspicious activity;
- Rules and regulations for reporting currency transactions, transportation of monetary instruments and suspicious activity;
- The Company's procedures for the internal and official reporting of unusual or suspicious activities;
- Civil and criminal penalties associated with money laundering;
- Changes in applicable laws, regulations and Company policies; and
- Any specific areas of importance to the Company, given its business and customer profiles.

This Anti-Money Laundering Compliance Program shall comprise a part of the training materials, and shall be presented to all new employees. Additional materials used in training will include:

- live presentations,
- on-line training programs,
- regulatory or governmental bulletins or alerts, and/or
- available C/E courses on the subject of AML.

The Company's training program as included herein will be updated as frequently as necessary to reflect recent developments, techniques or money laundering trends identified by various government agencies. The Company's goal is to maintain and provide a current, effective education service.

The AML Supervisor is responsible for ensuring that training of the Company's employees is conducted according to this training plan. The designated training staff will record the dates of training, employees trained and training methods used, and will present these records to the AML Supervisor for review and retention.

Reviewed by Richard Pound:

March 15, 2023