Abraham & Co., Inc.

Anti-Money Laundering (AML) Program: Compliance and Supervisory Procedures

Revised January, 2013

Introduction: Description of the Company

At this time, the Abraham & Co., Inc. (the "Company") conducts securities business in stocks, bonds, direct participation programs, IRA's, government bonds, margin accounts, money market funds, mutual funds, REITS, publicly traded limited partnerships, annuities and royalty/income trusts; it also performs advisory services and participates occasionally in private placements. Its clients consist of individuals, corporations and institutions. The Company clears all of its securities transactions (except private placements of unregistered securities) through its clearing firm, Southwest Securities, Inc., on a "fully disclosed" basis.

Currently, the Company is operated, managed and staffed by only one individual: Mr. Kye A. Abraham. All supervisory, compliance and other requirements described in this program shall be met by Mr. Abraham (the word 'we' used throughout this program refers to Mr. Abraham). In order to account for possible growth in staffing, the Company has chosen to leave intact text referring to the Company's infrastructure as if it consisted of more individuals than one.

Because Mr. Abraham is the founder and Compliance Officer as well as the Financial Operations Principal, he is keenly aware of the details relating to the Firm's business. By virtue of having to approve and sign all new accounts forms and monitor trading and order executions. Additionally Mr. Abraham receives copies of all customer emails to his personal computers. Records of Mr. Abraham's reviews exist in the form of his notes in customer records, his review of customer orders (email order instructions) weekly and monthly trade blotters, correspondence, and electronic records. Direct evidence of certain required reviews may not exist, due to the inherent redundancy of such records.

The Company operates under the "(k)(2)(ii)" exemption of Rule15c3-3, because it meets the following condition: The broker-dealer is an introducing broker-dealer who clears all transactions with and for customers on a fully-disclosed basis with a clearing broker or dealer, and who promptly transmits all customer funds and securities to the clearing broker or dealer which carries all of the accounts of such customers and properly maintains and preserves such books and records. Because the Company does not handle customer funds and does not accept cash, the likelihood of it enabling money launderers is considered slim; however, this fact does not diminish the importance of complying with AML Rules and Regulations.

1. Firm Policy

It is the policy of the Company to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three

stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

By adhering to the enclosed procedures, the Company's employees and associated persons will attempt to deter and detect money laundering activities by customers and 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. To follow is the Company's commitment statement. Each employee of Abraham & Co., Inc., by virtue of his or her employment by the Company, agrees to accept and abide by this Commitment Statement.

COMMITMENT STATEMENT

ABRAHAM & CO., INC. 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 THE FIRM 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.

Resources: NtM 02-21, page 5; SIA Preliminary Guidance for Deterring Money Laundering Activity ("SIA Guidance"), at pages 2-3 (Feb. 2002).

Rules: 31 C.F.R. § 103.120(c); FINRA Rule 3310.

2. AML Compliance Officer Designation and Duties

The Company has designated Kye Abraham as its **AML Compliance Officer.** Mr. Abraham is qualified by experience, knowledge and training, as the Company's founder and sole principal since 1983. Mr. Abraham is required to implement and monitor the day-to-day operations and internal controls of the Company's Anti-Money Laundering Program. The AML Compliance Officer's responsibilities are included throughout this AML Manual in detail. To follow is a summary of some of those responsibilities:

- Ensure that this AML Manual is distributed to all Company personnel.

- 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 Compliance Officer for guidance.
- Review any account or other activity deemed to warrant further investigation.
- Act as the initial and final point of authority in the process of determining whether or not certain unusual activities constitute reportable suspicious activities.
- When warranted, ensure Suspicious Activity Reports (SAR-SFs) are filed.
- Ensure that the requirements under Rule 3011 and any new, relevant rules and regulations are implemented on a continuing basis.
- Ensure that proper records are kept, in accordance with all applicable BSA and other regulatory requirements.
- Implement all additional procedures contained in this written program.

The Company will provide FINRA with contact information for the AML Compliance Officer, including name, title, mailing address, e-mail address, telephone number and facsimile number. As Executive Representative, Mr. Abraham will also, within 17 business days after the end of each calendar quarter, review and update, if necessary, the AML compliance person information. The Company will promptly notify FINRA of any change to this information.

Rules: 31 C.F.R. § 103.120; FINRA Rule 3310, NASD Rule 1160.
Resources: NTM 06-07; NTM 02-78. Firms can submit their AML Compliance Person information through FINRA's FCS Web page.

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

a. FinCEN Requests Under PATRIOT Act Section 314

Under Treasury's final regulations (published in the Federal Register on September 26, 2002), we will respond to a Financial Crimes Enforcement Network (FinCEN) request about accounts or transactions by immediately searching our records, at our head office or at one of our branches operating in the United States, to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity, or organization named in FinCEN's request. Upon receiving an information request, we will designate one person to be the point of contact regarding the request and to receive similar requests in the future (Mr. Abraham has been designated as such). Unless otherwise stated in FinCEN's request, we are required to search current accounts, accounts maintained by a named suspect during the preceding 12 months, and transactions conducted by or on behalf of or with a named subject during the preceding six months. If we find a match, we will report it to FinCEN by completing FinCEN's subject information form. This form can be sent to FinCEN by electronic mail at sys314a@fincen.treas.gov, by facsimile transmission to 703-905-3660. If the search parameters differ from those mentioned above (for example, if FinCEN requests longer periods of time or limits the search to a geographic location), we will limit our search accordingly.

If we search our records and do not uncover a matching account or transaction, then we will not reply to a 314(a) request.

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. We will maintain procedures to protect the security and confidentiality of requests from FinCEN, such as those established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act. In this regards, we do not intend to, nor are we required to, maintain copies of the actual lists reviewed; however, we will endeavor to maintain a record of having checked the lists. Such record may be in the form of notated ('flagged') e-mail notices of posted lists received from FinCEN.

We will direct any questions we have about the request to the requesting Federal law enforcement agency as designated in the 314(a) request.

Unless otherwise stated in the information request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the request as a list for purposes of the customer identification and verification requirements. We will not use information provided to FinCEN for any purpose other than (1) to report to FinCEN as required under Section 314 of the PATRIOT Act; (2) to determine whether to establish or maintain an account, or to engage in a transaction; or (3) to assist the Company in complying with any requirement of Section 314 of the PATRIOT Act.

Rule: 31 C.F.R. § 103.100.
Resources: FinCEN press release (2/6/03); FinCEN press release (2/12/03); NASD Member Alert (2/14/03); FinCEN's 314(a) Fact Sheet (11/18/08). FinCEN also provides financial institutions with General Instructions and Frequently Asked Questions relating to 314(a) requests through the 314(a) Secured Information Sharing System or by contacting FinCEN at (800) 949-2732.

b. Sharing Information With Other Financial Institutions

As an introducing firm, it is likely that, when warranted, we will share information about those suspected of terrorist financing and money laundering with our clearing firm or other financial institutions for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities and to determine whether to establish or maintain an account or engage in a transaction. Before any sharing occurs, we will file with FinCEN an initial notice and we will file annual notices thereafter. We will use the notice form found at FinCEN's Web site. 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 with respect to financial institutions *with whom we are affiliated*, and so we will obtain the requisite notices from affiliates and follow all required procedures.

As noted, we may share information about particular suspicious transactions with our clearing broker for purposes of determining whether one of us will file a SAR-SF. In cases in which we file a SAR-SF for a transaction that has been handled both by us and by our clearing broker, we may share with the clearing broker a copy of the filed SAR-SF, unless it would be inappropriate to do so under the circumstances, such as where we filed a SAR-SF concerning the clearing broker or one of its employees.

We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, including segregating it from the Company's other books and records. Only the AML Compliance Officer is permitted to access this information. See below for further procedures relating to the confidentiality of suspicious activity records.

Rules: FINRA Rule 3011; Section 314(b) of the PATRIOT Act; 31 C.F.R. §103.19; 31 C.F.R. § 103.110. Other Resources: The notice form can be found at http://www.fincen.gov/fi_infoappb.html. See: NtM 02-21, page 13.

4. Checking the Office of Foreign Assets Control ("OFAC") List

Before opening an account we will check to ensure that a customer does not appear on Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" List (SDN List) (*See* the OFAC Web Site at *www.treas.gov/ofac*, which is also available through an automated search tool on *http://apps.FINRA.com/Rules_&_Regulations/ofac/default.asp*), and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC website. In addition, the AML Compliance Officer or his or her designee is required to periodically check OFAC lists for the presence of existing account names. The Company's AML Compliance staff should regularly review the OFAC website; the Company may register with OFAC's e-mail subscription services to receive information and updates. By being familiar with OFAC's website, the AML Compliance staff will enhance its ability to promptly detect possible customer matches, thereby avoiding penalties for non-compliance. The Company must maintain evidence of its efforts to check OFAC lists for both new and existing account names (for instance, a log or an electronic record of searches).

If the individual conducting an OFAC search finds a match, he or she should conduct further internal due diligence to confirm that the match is a "true hit" and not a "false positive." In other words, he or she should confirm that a number of similarities exist—not just the name, for instance—BEFORE calling the OFAC hotline. 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 personnel confirm a match, they must report such to the AML Compliance Officer. He or she (or the CCO or legal counsel, if so determined) must immediately inform OFAC 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 of 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.

Other Resources: NtM 02-21, page 6, n.24;
SDN List- http://www.treas.gov/ofac/t11sdn.pdf.
The OFAC Web site -- http://www.treas.gov/ofac/t11facsc.pdf -- contains checklists and information for securities firms to follow in checking the OFAC list. You can subscribe to receive updates at http://www.treas.gov/press/email/subscribe.html.
FINRA provides a search engine to automate OFAC list searches at http://www.FINRAr.com/ofac/
Blocked Properties Reporting Form -- http://www.treas.gov/offices/enforcement/ofac/legal/forms/td902250.pdf.
Voluntary Form for Reporting Blocked Transactions – http://www.treas.gov/offices/enforcement/ofac/legal/forms/e_blockreport1.pdf.
Voluntary Form for Reporting Rejected Transactions – http://www.treas.gov/offices/enforcement/ofac/legal/forms/e_recjectreport1.pdf.

5. Customer Identification and Verification

In addition to the information we must collect under FINRA Rules 2110 (Standards of Commercial Honor and Principles of Trade), 2310 (Recommendations to Customers - Suitability), and 3110 (Books and Records), and SEC Rules 17a-3(a)(9) (Beneficial Ownership regarding Cash and Margin Accounts) and 17a-3(a)(17) (Customer Accounts), we have established, documented, and maintained a written Customer Identification Program (CIP). We will collect certain minimum customer **identification** information from each customer who opens an account; utilize risk-based measures to **verify** the identity of each customer who opens an account; **record** customer identification information and the verification methods and results; provide **notice** to customers that we will seek identification information and compare customer identification information with government-provided **lists** of suspected terrorists.

The Company intends to accept or solicit only those customers 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 customers and will only accept customers when this process has been completed.

Definitions. In the context of this CIP, "customer" refers to a person that 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. Not included are 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. Also not included are many categories of accounts, such as Federally-regulated financial institutions, banks, U.S. and State departments and agencies, and public companies with domestic operations. *Registered Representatives, if confused about whether or not a new customer falls under the definition of "customer" for CIP purposes, must consult the AML Compliance Officer for clarification.*

In the context of this CIP, "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, securities loan and borrow activity, and the holding of securities or other assets for safekeeping or

as collateral. The following are excluded from the definition of "account": (1) an account that the Company acquires through any acquisition, merger, purchase of assets, or assumption of liabilities, and (2) an account opened for the purpose of participating in an employee benefit plan established under ERISA. Transfers of accounts resulting from a change in clearing firm are also excluded. In general, customer-initiated transferred accounts are subject to CIP requirements.

a. Required Customer Information

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

- Name;
- Date of birth, for an individual;
- Address, which will be:
  - For an individual, a residential or business street address, or if neither exists, an Army Post Office or Fleet Post Office box number, or the residential or business street address of a next of kin or another contact individual; or
  - For an account other than an individual (such as a corporation, partnership, or trust), a principal place of business, local office, or other physical location; and
- An identification number, which will be:
  - For a U.S. person (individual or entity), a taxpayer ID number; or
  - For a non-U.S. person, one or more of the following:
    - A taxpayer ID number;
    - A passport number and country of issuance;
    - An alien identification card number; or
    - The number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

This minimum information must be gathered PRIOR to opening the account; however, If a customer has applied for, but has not received, a taxpayer ID number at the time of account opening, RR's are permitted to open the account if they document in the customer's file records the circumstances, including the following: the reason for the lack of ID number; the expected time frame for receipt of the ID number; and all efforts made by the RR to obtain the ID number (such as contacting the customer on or about the estimated receipt date and frequently thereafter). If the ID number is not received within 60 days after the estimated receipt date, the account must be closed (unless the AML Compliance Officer extends this deadline based on reasonable factors).

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.

Rules: FINRA Rule 3011; Section 326 of the PATRIOT Act; 31 C.F.R. §§103.122 et seq. See: NtM 02-21-, NtM 02-50, pages 5-7.

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 Company will

not open a new account and, after considering the risks involved, will consider closing any existing account. In either case, the AML Compliance Officer will be notified so that we can determine whether we should report the situation to FinCEN (i.e., file a Form SAR-SF).

See NtM 02-21, page 7.

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. In verifying customer identity, we will analyze any logical inconsistencies in the information we obtain.

The Company is not required to verify the identities of individuals with authority or control over accounts (of non-individuals, for example) on which they are not named as accountholders. However, in the event insufficient verification is available to identify such accounts, RR's must attempt to obtain information on the individuals with authority or control over these accounts. Failed attempts are valid reasons for not opening accounts, in such situations.

We will verify customer identity through documentary evidence, non-documentary evidence, 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 deemed necessary. We may also use such non-documentary means, after using documentary evidence, if we are still uncertain about whether we know the true identity of the customer. In analyzing the verification information, we will consider whether there is a logical consistency among the identifying information provided, such as the customer's name, street address, zip code, telephone number (if provided), date of birth, and social security number.

Appropriate documents for verifying the identity of customers include, but are not limited to, the following:

- 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 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:

- Contacting a customer at the contact numbers/address provided;
- 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 in the following situations: (1) when the customer 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 customer presents for identification verification; (3) when the customer 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 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 or terrorist financing activity, we will, after internal consultation with the Company's AML Compliance Officer, file a SAR-SF in accordance with applicable law and regulation.

Additional Information Gathering:
Registered Representatives, in opening new accounts, must attempt to obtain the minimum information described above. In addition, certain other information may be required in order to meet suitability obligations and to firmly establish the identity and source of funds for each account. These other information requirements are described below and vary according to according to the type of account.

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 RR's are uncertain about the information required to verify the identity of any given customer, they should immediately contact their designated supervisors or the AML Compliance Officer 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 in this program. In addition, throughout the information gathering process, RR's and designated supervisors should make notes on their questions, concerns or suspicions, and include those notes in the respective account files. Suspicions raised should be reported internally according to the process described below under "Suspicions at the Account Opening Stage."

1) **Individual Accounts**—In accordance with the Company's written supervisory procedures and to meet suitability and other regulatory standards, Registered Representatives must make reasonable efforts to obtain the following, additional information prior to opening an account or commencing a business relationship: the customer's date of birth, investment objectives and experience, if applicable, net worth, annual income, occupation and employment data; and names of all authorized persons. In the case of "confidential accounts," maintained for appropriate reasons

such as the customer's prominence or due to concerns for personal safety, sufficient documentation identifying the underlying owner(s) (as described in this paragraph and in subsequent paragraphs, where applicable) must be obtained and on file, available to designated compliance staff.

2) **Non-Resident Alien Accounts**—In addition to the minimum information required and the information gathered under number 1 above, if the customer is a non-resident alien, the Registered Representative must obtain all necessary U.S. tax forms. If the individual's country of origin is listed on OFAC, the RR should get approval from the AML Compliance Officer prior to opening the account. Due diligence may be required; if conducted, notes to the customer's files should made for future reference.
3) **Accounts Opened via the Internet—**All account opening and review procedures listed here apply equally to those accounts opened online. The Company's existing requirements for opening and approving online accounts must be followed as part of these AML procedures. Should the RR or his or her supervisor determine the need for more information on an existing or prospective customer, s/he should contact the customer to request and obtain such information. In the event the customer is not willing to provide requested information or is unable to be contacted, the RR or supervisor should consult the AML Compliance Officer in order to request the use of outside vendors or public information sources for the purpose of gathering the necessary, clarifying information. The AML Compliance Officer may determine that the use of such sources is ill-advised, and may instead not approve the opening (or continuation) of such account, given the lack of disclosure.
4) **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 (by receiving a corporate resolution granting authority). If doubt exists or risk is perceived, the RR must obtain information sufficient to confirm the identity and authority. New customers that are LLC's 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.
5) **Domestic Trusts and Omnibus Accounts**—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. Similarly, for omnibus accounts, the RR must identify the intermediary if the intermediary is the named accountholder (i.e., the RR is not obligated to identify the underlying beneficial owners).
6) **Institutional or Intermediary Accounts, Such as Hedge Funds, Investment Funds and Other Intermediaries—**While not usually representing a credit risk to the Company, these types of accounts may enable money launderers and therefore represent risk in another form. Therefore, it is necessary to apply scrutiny to institutional accounts. The Company's existing procedures related to suitability (based on FINRA Rule IM-2310) and account documentation (Rule 3110) must be followed, as well as the guidance provided in the other topics listed here). In order to determine whether or not further due diligence is necessary when opening a new institutional account or continuing to do business with one, RR's and their supervisors should 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 an FATF jurisdiction;
- The institution/intermediary has a reputable history in the investment business; and/or
- The institution/intermediary is not from a jurisdiction characterized as an offshore banking or secrecy haven or 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 Manual, the RR may wish to receive written acknowledgement or confirmation of some of the topics above. Registered Representatives should be aware that institutional accounts 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 RR's supervisor, 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.

7) **Foreign Operating Commercial Entities, Personal Investment Corporations or Personal Holding Companies and Offshore Trusts**—Should the Company have foreign entities as customers, the account Representative must endeavor to accumulate as much information on the customer as is required for all customers—including an understanding of the beneficial ownership of such entity. In addition, various factors should be considered, such as the entity's country of incorporation and the foreign or offshore jurisdiction in which the business is located and if the entity has been established by, or for the benefit of, a senior foreign public official (see below). The RR must be particularly thorough in gathering account documentation, due to the inherent heightened risk of disguised intent.
8) **Private Banking Accounts for Non-U.S. Persons/Senior Foreign Public Officials**—see below for specifics.
9) **Correspondent Accounts for Foreign Financial Institutions**—see below for specifics.

Additional Due Diligence:

There may be instances where more information is required for the Company to meet its "Know Your Customer" and identity/source of funds standards. Specific due diligence requirements relating to certain account types, such as Private Banking Accounts for non-U.S. persons, including Senior Foreign Political Figures, and Correspondent Accounts for certain foreign financial institutions, are described below, if applicable. Other reasons for additional due diligence may exist—for instance to resolve a perceived discrepancy in a customer's tax ID number, date of birth, residential address, etc.

If questions remain after personnel have made effort to authenticate customers' identities and apparent funding sources, these questions should be presented to the AML Compliance Officer who may decide to make use of the following tools 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).

Further research will be required if personnel suspect that an account is located or incorporated in certain countries or regions identified as non-cooperative with international anti-money laundering principles/procedures or having inadequate anti-money laundering measures. In this case, the AML Compliance Officer may consult one of more of the following sources 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.

The individual(s) performing any such additional due diligence must document those efforts and include all related information in the customer's file. This information, if indicative of suspicious activity, should be placed in a dedicated file to remain confidential and should be used to substantiate in-house or regulatory reporting, described below.

The Company, in applying any such additional measures, will comply with all privacy requirements unless such requirements are exempted by a federal authority.

See: NtM 02-21, pages 6-7.

d. Lack of Verification

As described above, the Company requires its personnel to attempt to verify the identities of new customers prior to or upon account opening; however, verification of identity may take place AFTER account opening. The RR should apply a risk-based analysis in order to determine the best timing for verification. For instance, if a new customer is completely unknown to the Company and the RR, or could be construed to represent higher risk (based on the specific account profile, as described below), verification of identity should take place before the account is opened. If, given the nature of a new customer (such as how s/he or it was introduced to the RR--by a trusted associate, for example), the RR believes s/he knows the true identity of the customer, verification may take place after account opening. RR's unsure of how to proceed should discuss the account with their supervisors.

In instances where verification has not occurred before account opening, the AML Compliance Officer must consider the nature of the account and the type(s) of requested transactions before they approve any new business for the account. The AML Compliance Officer has the right and

the obligation to prohibit or restrict trade or other activity in new accounts if verification is lacking and considered mandatory to knowing the true identity of a new customer. In general, the Company prohibits trade activities in accounts where identity has not yet been verified. Despite thisgeneral guidelines, the AML Compliance Officer may use discretion in allowing unlimited account activity to proceed in certain unverified accounts, if deemed appropriate and not outside acceptable risk tolerances. RR's with questions as to allowable trade activity in unverified accounts should consult the AML Compliance Officer for guidance.

If efforts to verify the identity of the customer fail after 30 days after opening the account such account must be closed. If verification efforts fail prior to opening the account because of the apparent lack of cooperation of the customer, the account must not be opened. In either of these cases, the Registered Representative must report such failure to the AML Compliance Officer, who will then determine if filing a SAR-SF is merited.

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 discrepancy in the identifying information. We will keep records containing a description of any document (not necessarily the document itself) 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 maintain 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.

Rule: 31 C.F.R. §103.122(b)(3).

f. Comparison with Government Provided Lists of Terrorists and Other Criminals

From time to time, we may receive notice that a Federal government agency has issued a list of known or suspected terrorists. 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), we 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 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 with Treasury's Office of Foreign Asset Control rules prohibiting transactions with certain foreign countries or their nationals.

See NtM 02-21, page 6. *Other Resources: NtM 02-21, page 6, n.24; 31 C.F.R. §§ 103.122.*

g. Notice to Customers

BEFORE an account is opened or trading authority granted, the Company must provide notice to customers that it is requesting information from them to verify their identities. The Company will provide notification, making use of required language (see below), as follows: Registered Representatives are required to orally describe the identification requirements to each and every

customer for whom they open new accounts, whether during telephone or face-to-face discussions.

The following language or a version thereof should be used to notify customers of the Company's obligation:

> **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 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.**

The Company may also make use of a notice prepared by the FINRA in order to fulfill this notification requirement. The form of notice is available at: FINRA's AML Web page

Rule: 31 C.F.R. §103.122(g).

h. Reliance on Another Financial Institution for Identity Verification

If the following criteria are met, the Company is permitted to rely on one or more financial institutions to perform some or all of the elements of its customer identification program 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:

- Such reliance is reasonable under the circumstances;
- 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
- 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.

If the Company intends to rely on an entity such as a hedge fund manager or investment advisor to identify customers introduced by the Company to a transaction, the other entity must be regulated by a Federal functional regulator (i.e., registered with the S.E.C.) and must have an AML Program in place. Any such agreement should be described in writing and renewed annually. *No exemptions from CIP requirements currently exist for private placement and hedge fund offerors: identification and verification must take place for customers, as defined.*

The Company does not currently rely on another financial institution to assist in its CIP efforts.

Rule: 31 C.F.R. §§ 103.122 et seq.

6. Foreign Correspondent Accounts and Foreign Shell Banks

a. Detecting and Closing Correspondent Accounts of Unregulated Foreign Shell Banks

The Company does not permit the opening of correspondent accounts for foreign financial institution, including banks. If the RR, his/her supervisor or the AML Compliance Officer determines that, based on account research efforts (as described herein), a correspondent account has been opened for a foreign financial institution, as defined, the AML Compliance Officer is required to take steps necessary to close the account. If the account is permitted to remain open (with the noted approval of the AML Compliance Officer), the Company must establish and apply required due diligence procedures to the account (and include a description of those procedures herein). All Company employees and associated persons must report to the AML Compliance Officer any perceived attempt on behalf of a customer to open such an account with the Company. The AML Compliance Officer must then investigate the known circumstances of the attempt in order to determine if suspicion exists; if so, he or she must follow-up with actions designed to fulfill any and all reporting obligations.

The Company and its RR's are not permitted to establish, maintain, administer or manage a correspondent account in the U.S. for, or on behalf of, a prohibited foreign shell bank (generally meaning, a foreign bank that does not have a physical presence in any country and is not a "regulated affiliate" as defined by the Treasury). Upon finding or suspecting such accounts, Company employees will notify the AML Compliance Officer, who will terminate any verified correspondent account in the United States for an unregulated foreign shell bank. We will also terminate any correspondent account that we have determined is not maintained by an unregulated foreign shell bank but is being used to provide services to such a shell bank. We will exercise caution regarding liquidating positions in such accounts and take reasonable steps to ensure that no new positions are established in these accounts during the termination period.

Rules: 31 C.F.R. §§103.175, 103.177.

b. Certifications

Because the Company does not permit this type of account, procedures for filing completed "Certifications for Purposes of Sections 5318(K) of Title 31, U.S. Code" have *not* been made effective. However, should such accounts be allowed in the future, the following procedure will apply: We will require our foreign bank account holders to complete model certifications issued by the Treasury. We will send the certification forms to our foreign bank account holders for completion, which requires them to certify that they are not shell banks and to provide ownership and agent information. We will re-certify when we believe that the information is no longer accurate and at least once every three years.

Rules: FINRA Rule 3011; Section 313 of the PATRIOT Act; 31 C.F.R. §§103.175 et seq.

c. Recordkeeping for Foreign Correspondent Accounts

Because the Company does not permit this type of account, procedures for maintaining required records have *not* been made effective. However, should such accounts be allowed in the future, the following procedure will apply: We will keep records identifying the owners of foreign banks with U.S. correspondent accounts and the name and address of the U.S. agent for service of legal process for those banks.

Rules: FINRA Rule 3011; Sections 313 and 319 of the PATRIOT Act; 31 C.F.R. §§ 103.175, 177.

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

While the following procedures may not apply due to the Company's lack of correspondent accounts, they are important to evidencing the Company's willingness to cooperate with federal law enforcement. Should we ever receive a written request from a federal law enforcement officer for information concerning correspondent accounts, we will provide that information to the requesting officer not later than 7 days after receipt of the request. We will close, within 10 days, any account for a bank that we learn from Treasury or the Department of Justice has failed to comply with a summons or has contested a summons. We 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.

Rules: FINRA Rule 3011; Sections 313 and 319 of the PATRIOT Act; 31 C.F.R. § 103.185.

7. Private Banking Accounts/Foreign Officials

A private banking account is one that is established or maintained for the benefit of one or more persons, *requires* a minimum aggregate deposit of funds or other assets of not less than $1,000,000, and is assigned to an officer, employee or agent of a financial institution (here, the Company) who acts as the liaison between the financial institution and the person. *The Company does not permit the opening of private banking accounts for non-U.S. persons.* All Company employees and registered persons must report to the AML Compliance Officer any perceived attempt on behalf of a customer to open such an account with the Company. Should such an attempt be detected, the AML Compliance Officer will investigate and follow-up with actions designed to halt the activities and fulfill any and all reporting obligations.

A "senior foreign political figure" is: a current or former senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government, whether or not they are or were elected officials; a senior official of a major foreign political party; and a senior executive of a foreign government-owned commercial enterprise. This definition also includes a corporation, business, or other entity formed by or for the benefit of such an individual. Senior executives are individuals with substantial authority over policy, operations, or the use of government-owned resources. Also included in the definition are immediate family members of such individuals, and those who are widely and publicly known (or actually known) close associates of a senior foreign political figure. *The Company does not permit the opening of Private Banking Accounts for Senior Foreign Political Figures.* If the RR, his or her supervisor or The AML Compliance Officer determines that, based on account research efforts (as described herein), a private banking account has been opened for a senior foreign political figure, as defined, the AML Compliance Officer is required to take steps necessary to close the account. If the account is permitted to remain open (with the noted approval of the AML Compliance Officer), the Company must establish and apply enhanced scrutiny procedures to the account (and must include a description of those procedures herein). All Company employees and associated persons must report to the AML Compliance Officer any perceived attempt on behalf of a customer to open such an account with the Company. The AML Compliance Officer must then investigate the known circumstances of the attempt in order to determine if suspicion exists; if so, he or she must follow-up with actions designed to fulfill any and all reporting obligations.

Rules: 31 C.F.R. § 103.120; FINRA Rule 3310.

Resource: *NTM 06-07*.

8. Monitoring Accounts For Suspicious Activity

Because Mr. Abraham is the sole individual conducting business on behalf of the Company, he is keenly aware of the details relating to that business. By virtue of having been party to every transaction of the Company from start to finish, Mr. Abraham considers himself to have reviewed and monitored all account activity. Mr. Abraham's manual, daily monitoring of account activity is expected to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as "non-cooperative" are involved, and any of the "red flags" identified in Section 8b below. He will look at transactions, including wire transfer requests (the Company itself does not execute wire transfers, but does forward requests to its clearing firm), in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that customer. Account review and transaction monitoring efforts will be documented as described in the Company's WSP Manual. Our AML Compliance Officer will conduct an appropriate investigation before a SAR is filed. The AML Compliance Officer will report suspicious activities to the appropriate authorities, when warranted. Among the information the AML Compliance Officer will use to determine whether to file a Form SAR-SF are various exception and other reports provided by the Company's clearing firm that may include transaction size, location, type, number, and nature of the activity. When deemed necessary, the Company will create lists of high-risk clients whose accounts may warrant further scrutiny.

See NtM 02-21, pages 9-12.

a. Emergency Notification to the Government by Telephone

When conducting due diligence or opening an account, we will immediately call Federal law enforcement when necessary, and especially in these emergencies: a legal or beneficial account holder or person with whom the account holder is engaged in a transaction is listed on or located in a country or region listed on the OFAC list, an account is held by an entity that is owned or controlled by a person or entity listed on the OFAC list, a customer tries to use bribery, coercion, or similar means to open an account or carry out a suspicious activity, we have reason to believe the customer is trying to move illicit cash out of the government's reach, or we have reason to believe the customer is about to use the funds to further an act of terrorism. We will first call the OFAC Hotline at 1-800-540-6322. The other contact numbers we will use are: Financial Institutions Hotline (1-866-556-3974), local U.S. Attorney's Office (253-428-3800), local FBI Office (206- 622-0460), and local SEC Office (206- 220-7500).

Other Resources: *SDN List -- http://www.treas.gov/ofac/t11sdn.pdf. . See: NtM 02-21, page 13.*

b. Red Flags

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

- The customer exhibits unusual concern about the Company's compliance with government reporting requirements and the Company's AML policies (particularly concerning his or her identity, type of business and assets), or is reluctant or refuses to

reveal any information concerning business activities, or furnishes unusual or suspicious identification or business documents.

- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business or investment strategy.

- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.

- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.

- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.

- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.

- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.

- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.

- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from the Company's policies relating to the deposit of cash.

- The customer engages (or wishes to engage) in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.

- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.

- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the FATF.

- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.

- The customer's account shows numerous currency or cashiers check transactions aggregating to significant sums.

- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.

- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven.

- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.

- 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.

- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.

- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.

- The customer requests that a transaction be processed to avoid the Company's normal documentation requirements.

- 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.)

- The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.

- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose.

- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

c. Responding to Red Flags and Suspicious Activity

Registered Representatives, back office and administrative personnel and their supervisors must be familiar with these indicators and must make note of them, if perceived. When a member of the Company detects any red flag he or she must report such to the AML Compliance Officer, who will direct any subsequent investigation, if he deems it necessary. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account, or filing a Form SAR-SF.

9. Suspicious Transactions and BSA Reporting

a. Filing a Form SAR-SF; Confidentiality; Recordkeeping; Response to Subpoenas

We will file Form SAR-SFs for any account activity (including deposits and transfers) conducted or attempted through our Company involving (or in the aggregate) $5,000 or more of funds or assets 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 the 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 we know, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the transaction, or 4) the transaction involves the use of the Company to facilitate criminal activity.

We will not base our decision on whether to file a SAR-SF solely on whether the transaction falls above a set threshold. We will file a SAR-SF and notify law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities. In high-risk situations, we will notify the government immediately (see Section 8 for contact numbers) and will file a SAR-SF with FinCEN. Securities law violations that are reported to the SEC or a Self-Regulatory Organization (SRO) may also be reported promptly to the local U.S. Attorney, as appropriate.

We will not file SAR-SFs to report violations of Federal securities laws or SRO rules by our employees or registered representatives that do not involve money laundering or terrorism, but we will report them to the SEC or SRO (here, the FINRA).

While all SAR-SFs require reporting to the Board of Directors and senior management, the Company currently has no such senior management besides Mr. Abraham, who will ensure confidentiality of the SAR-SF.

We will report suspicious transactions by completing a SAR-SF 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-SF. If no suspect is identified on the date of initial detection, we may delay filing the SAR-SF for an additional 30 calendar days pending identification of a suspect, but in no case, will the reporting be delayed more than 60 calendar days after the date of initial detection.

We will retain copies of any SAR-SF filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR-SF. We will identify and maintain supporting documentation and make such information available to FinCEN, any other appropriate law enforcement agencies, or federal or state securities regulators, 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-SF or the information contained in the SAR-SF, except where disclosure is requested by FinCEN, the SEC, or another appropriate law enforcement or regulatory agency or an SRO registered with the SEC, will decline to produce to the SAR-SF or to provide any information that would disclose that a SAR-SF was prepared or filed. We will notify FinCEN of any such request and our response.

Rules: FINRA Rule 3011; Section 356 of the PATRIOT Act; 31 C.F.R. §103.19.
Other Resources: FinCEN's Web Site contains additional information (See www.fincen.gov), including annual SAR Activity Reviews and SAR Bulletins, which discuss trends in suspicious reporting and give helpful tips. NTM 02-21, page 12, n.38; NtM 02-47. See: NtM 02-21, pages9, 10, 11-12; NtM 02-47.

SAR-SF Form (fill-in version) -- http://www.fincen.gov/fin101_formandinstructions.pdf
http://www.fincen.gov/fin101_form_only.pdf
SAR Activity Reviews -- http://www.fincen.gov/pub_main.html
SAR Bulletins -- http://www.fincen.gov/pub_main.html

b. Currency Transaction Reports (CTR)

Our firm prohibits the receipt of currency and has the following procedures to prevent its receipt: In the event cash is mistakenly received from a customer, it must be recorded in the cash receipts blotter before being returned promptly to the client and respective RR or designated operations staff must then notify the client of its policy to not receive cash. The Company's AML Compliance Officer must be informed of the event. If we discover currency exceeding $10,000 has been received, we will file with FinCEN a CTR. Multiple transactions will be treated as a single transaction if they total more than $10,000 during any one business day. We will use the CTR form at http://www.fincen.gov/reg_bsaforms.html#4789.

Rules: 31 C.F.R.§§103.11, 103.22

c. Currency and Monetary Instrument Transportation Reports (CMIR)

Our firm prohibits the receipt of currency and has the procedures described in the previous subsection to prevent its receipt. If we discover currency has been received, we will file with the Commissioner of Customs a CMIR whenever the Company transports, mails, ships or receives or causes or attempts to transport, mail, ship or receive monetary instruments of more than $10,000 at one time (on one calendar day or, if for the purposed of evading the reporting requirements, on one or more days) in or out of the U.S. We will file a CMIR for all such shipments or receipts of monetary instruments, except for currency or monetary instruments shipped or mailed through the postal service or by common carrier. We will, however, file a CMIR for such receipts of currency and monetary instruments and for shipments and deliveries made by the Company by means other than the postal service or common carrier, even when such shipment or transport is made by the Company to an office of the Company located outside the U.S. We will use the CMIR Form at *http://www.fincen.gov/reg_bsaforms.html#4790*.

Rules: 31 C.F.R. §§103.11, 103.23.

d. Foreign Bank and Financial Accounts Reports (FBAR)

We will file with FinCEN an 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 FBAR Form at *http://www.fincen.gov/f9022-1.pdf*.

Rules: 31 C.F.R. §103.24.

e. Transfers of $3,000 or More Under the Joint and Travel Rule

When we transfer funds of $3,000 or more, we will record on the transmittal order at least the following information: the name and address of the transmitter and recipient, the amount of the transmittal order, the identity of the recipient's financial institution, and the account number of the recipient. We will also verify the identity of transmitters and recipients who are not established customers of the Company (i.e., customers of the Company who have 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). Because the Company does not execute wire transfers for customers, but rather, forwards wire transfer requests to its clearing firm, the Company expects that it is the clearing firm who will record and maintain required wire transmittal order information, as described above.

Rules: 31 C.F.R. §103.33(f)

10. AML Record Keeping

a. SAR-SF Maintenance and Confidentiality

We will hold SAR-SFs and any supporting documentation confidential. We will not inform anyone outside of a law enforcement or regulatory agency or securities regulator about a SAR-SF. We will refuse any subpoena requests for SAR-SFs or SAR-SF information and immediately tell FinCEN of any such subpoena we receive. We will segregate SAR-SF filings and copies of supporting documentation from other firm books and records to avoid disclosing SAR-SF filings. Our AML Compliance Officer will handle all subpoenas or other requests for SAR-SFs. As describe in detail above, we may, when appropriate, share information with our clearing broker about suspicious transactions in order to determine when a SAR-SF should be filed and we may share with the clearing broker a copy of the filed SAR-SF – unless it would be inappropriate to do so under the circumstances, such as where we file a SAR-SF concerning the clearing broker or its employees.

Rules: 31 C.F.R. §103.19; 67 Fed. Reg. 126, 44501-44502 (July 1, 2002). See: NtM 02-21, page 12.

b. Responsibility for AML Records and SAR Filing

The AML Compliance Officer will ensure that all records required to be kept per BSA, SEC, FINRA, U.S. Treasury and other regulatory or governmental body rules will be made and maintained in accordance with those rules. Our AML Compliance Officer will be responsible to ensure that SARs are filed as required.

See: NtM 02-21, page 14.

c. Records Required

As part of our AML program, our firm will create and maintain SAR-SFs, CTRs, CMIRs, FBARs, and relevant documentation on customer identity and verification (see Section 5 above) and funds transfers and transmittals as well as any records related to customers listed on the OFAC list. We will maintain SAR-SFs and their accompanying documentation for at least five years. We will keep other documents according to existing BSA and other record keeping requirements, including certain SEC rules that require six-year retention.

Rules: FINRA Rule 3011; 31 C.F.R. §103.19; 31 C.F.R. §103.33(f).

11. 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. (A description of information sharing under 314(b) is described above in Section 3b.) As a general matter, we have agreed that our clearing firm will monitor customer activity on our behalf, and we will provide our clearing firm with proper customer identification information as required to successfully monitor customer transactions. We have allocated these functions and set them forth in a written document. (see "Amendment To Fully Disclosed Clearing Agreement Regarding Patriot Act And Anti-Money Laundering Initiatives" dated July 28, 2005) We understand that the allocation of functions will not relieve either of us from our independent obligation to comply with AML laws, except as specifically allowed under the PATRIOT Act and its implementing regulations.

Rules: FINRA Rule 3011; Sections 314(b) and 352 of the PATRIOT Act; Section 3.b. above. See NtM 02-21, page 15.

12. Training Programs

We will develop ongoing employee training under the leadership of the AML Compliance Officer 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. Currently, due to the Company's small size (one person firm), training will consist of Mr. Abraham's review of new announcements made via FINRA's website and other news encountered in the context of his keeping abreast of securities regulation. Mr. Abraham will endeavor to remain aware of and informed on the following subjects: how to identify red flags and signs of money laundering that arise during the course of the his duties; what to do once the risk is identified; what his roles are in the Company's compliance efforts and how to perform them; the Company's record retention policy; and the disciplinary consequences (including civil and criminal penalties) for non-compliance with the PATRIOT Act.

Specific training tools used by Mr. Abraham may include regulatory or governmental bulletins or alerts, FINRA's E-Learning Courses and webcasts, and/or available outsourced C/E courses on the subject of AML. He will satisfy this training requirement no less frequently than annually. New employees are required to undergo AML training within one month of their hiring and annually, thereafter. Such training will consist of dedicated instruction provided by the AML Compliance Officer and may also include FINRA's E-Learning or other C/E Courses. We will maintain records to show the persons trained, the dates of training, and the subject matter of their training.

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

Rules: FINRA Rule 3011; Section 352 of the PATRIOT Act.

13. Program to Test AML Program

Goals. Compliance with these AML procedures will be tested periodically to determine their completeness and efficacy. In general, the purpose of testing is to assess the adequacy of the written program and to assess the extent to which Company personnel are complying with it. The

testing should incorporate an on-site records review designed to meet the following, general goals:

- The Company's written **procedures** are adequate to meet current FINRA and federal (BSA and its implementing regulations) requirements; that they have been made effective and that they are periodically updated when necessary;
- Company personnel are **complying** with the Company's written AML procedures and there are **records** to evidence this (maintained for required time period);
- The Company is **reporting** all reportable transactions in accordance with internal and federal directives;
- The Company is conducting AML **training** of its employees;
- The Company is conducting periodic **testing** of its AML program and is taking steps to implement changes to rectify noted deficiencies.

The results of independent testing must be reported to the AML Compliance Officer in a written report. The AML Compliance Officer must present all reports to the senior management of the Company (currently, only Mr. Abraham). The results of testing will alert the Company's senior management to any deficiencies in the Company's AML procedures and implementation and will allow the Company to take necessary corrective and/or disciplinary action. In general, periodic reviews and testing will be used as a basis for improving compliance with the AML procedures. The CCO shall ensure that corrective measures are taken when necessary and that copies of all reports of findings are maintained for a period of no less than five years.

Frequency. The Company's AML Program will be tested by an independent third party once every calendar year.

Appointed Independent Reviewer to Test AML Program. The testing of our AML program will be performed at least annually (on a calendar year basis) by Malone Bailey, LLP an independent third party. Malone Bailey has extensive working knowledge of applicable requirements under the BSA and its implementing regulations. As independent auditors and CPAs, Malone Bailey also has considerable experience in small firm (FINRA) accounting and reporting. Contact information is:

Malone Bailey, LLP
10350 Richmond Ave, Ste. 800
Houston, TX 77042
(713) 343-4200

Independent testing will be performed more frequently if circumstances warrant.

As a general matter, independent testing of the Company's AML compliance program should include, at a minimum: (1) evaluating the overall integrity and effectiveness of your firm's AML compliance program; (2) evaluating your firm's procedures for BSA reporting and recordkeeping requirements; (3) evaluating the implementation and maintenance of your firm's CIP; (4) evaluating your firm's customer due diligence requirements; (5) evaluating your firm's transactions, with an emphasis on high-risk areas; (6) evaluating the adequacy of your firm's staff training program; (7) evaluating your firm's systems, whether automated or manual, for identifying suspicious activity; (8) evaluating your firm's system for reporting suspicious activity; (9) evaluating your

firm's policy for reviewing accounts that generate multiple SAR-SF filings; and (10) evaluating your firm's response to previously identified deficiencies.

The Company has appointed Kye Abraham, the sole employee of the Company, to conduct periodic testing of its AML program. This individual has working knowledge of the applicable Bank Secrecy Act requirements and related implementing regulations, as required in IM-3011-1, but, because the Company is a small firm, it does not have internal personnel meeting the other criteria under the Rule. Therefore, it has appointed an individual (the "reviewer") to conduct AML testing who does indeed perform AML functions. The following is true in this circumstance:

- The Company has no other qualified personnel to conduct testing;
- The following policy applies: the reviewer is entitled to conduct his or her reviews and testing in an environment free of the threat of retaliation. Mr. Abraham has determined that, based on his 20+ years of proven integrity in operating a broker-dealer, the established AML testing process is adequate to meet the spirit of the Rule. Should Mr. Abraham determine that this testing arrangement is not adequate, the Company will appoint a qualified outside party to perform the required testing; and
- When possible, the results of testing will be reported to an individual senior to the person to whom the reviewer reports. However, currently, the Company cannot meet this requirement because the reviewer is the most senior person in the Company.

These points represent the rationale for the Company's choice to comply with IM-3011-1(c) in this manner. The Company considers this rationale reasonable. Should the Company's infrastructure change to the extent that it later meets all the independence standards under the Rule, then the CCO will ensure that the Company appoints a reviewer meeting these standards and these procedures and this rationale will be revised accordingly.

Rules: FINRA Rule 3011; IM-3011-1; NtM 06-07; Section 352 of the PATRIOT Act.

14. Monitoring Employee Conduct and Accounts

The Company does not maintain employee brokerage accounts. Outside brokerage accounts are reviewed as described in the Company's WSP Manual. Since Mr. Abraham is the sole principal of the Company, he reviews his own account activity for regulatory and AML compliance.

Rules: FINRA Rule 3011; Section 352 of the PATRIOT Act.

15. Confidential Reporting of AML Non-Compliance

Employees will report any violations of the Company's AML compliance program to the AML Compliance Officer, unless the violations implicate the Compliance Officer, in which case the employee shall report to the Company's independent financial auditor or FINRA District office (for guidance). Such reports will be confidential, and the employee will suffer no retaliation for making them.

Rules: FINRA Rule 3011; Section 352 of the PATRIOT Act.

16. Additional Areas of Risk

The Company has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above and does not believe there are any major additional areas of risk.

17. Senior Manager Approval

I have approved this AML program as reasonably designed to achieve and monitor our Company's ongoing compliance with the requirements of the BSA and the implementing regulations under it.

Signed: (See separate signature page dated 10-27-12)

Title:

Date:

These procedures are effective from the date approved until the date of their authorized revision, update or replacement.

[Date these procedures were replaced: _____]

Rules: *FINRA Rule 3011.*