Level Four Financial, LLC

Anti-Money Laundering Compliance Program Manual

April, 2025

Table of Contents

These Anti-Money laundering compliance procedures were approved by Kimberly Miller, AMLCO. These procedures are effective from the date approved until the date of their authorized revision, update or replacement (see below).

Authorized Approval Signature: _____ Date: _____

ANTI-MONEY LAUNDERING (AML) COMPLIANCE PROGRAM

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, Level Four Financial, LLC (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 Level Four Financial, LLC, 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 is registered as a Capital Acquisition Broker ("CAB"), 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);
> (d) 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
> (e) Provide ongoing training for appropriate personnel."

The Company's customers may include US publicly-traded companies, US or foreign private business entities, other broker/dealers, federally-regulated institutions, such as banks, US or foreign individuals.

COMMITMENT STATEMENT

LEVEL FOUR FINANCIAL, LLC 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 LEVEL FOUR FINANCIAL, LLC 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 Level Four Financial, LLC, by virtue of his or her employment by the Company, agrees to accept and abide by this Commitment Statement.

Outside brokerage accounts of Company personnel are monitored for AML related matters by the brokerage firms holding these accounts. However, the Company will also review these accounts in accordance with the procedures described in the Company's WSP Manual. In-house brokerage accounts of the Company's registered and unregistered personnel will be subject to the same AML identifying and monitoring procedures as customer accounts.

DEFINITIONS

Money Laundering: The process of disguising the origins of illicit funds through financial transactions in order to make the money appear legitimate. Broker-dealers may be used at the layering or integration stages.
Terrorist Financing: The act of providing or collecting funds with the intention that they be used to carry out terrorist acts. These funds can come from both legal and illegal sources.
Know Your Customer (KYC): The obligation to verify the identity of customers and understand the nature of their accounts and expected activity. A broker-dealer must collect identifying information and ensure it is accurate and complete.
Customer Due Diligence: Procedures used to obtain information about a customer's identity and assess the risk they pose. Includes developing a customer risk profile to identify unusual or suspicious behavior.
Enhanced Due Diligence: Additional scrutiny required for high-risk accounts, such as those involving PEPs, foreign financial institutions, or accounts with complex or opaque ownership structures.
Customer Identification Program: A program required under the USA PATRIOT Act, mandating broker-dealers to collect and verify information (name, DOB, address, identification number) for individuals opening new accounts.
Beneficial Owner: For legal entities, the natural person(s) who directly or indirectly owns 25% or more of the equity interests, or who exercises significant control over the entity. Broker-dealers are required to identify and verify these individuals.
Suspicious Activity Report (SAR): A report filed with the Financial Crimes Enforcement Network (FinCEN) when a transaction (or attempted transaction) involves $5,000 or more and is suspected to involve funds derived from illegal activity or designed to evade AML laws.
Office of Foreign Assets Control (OFAC): A U.S. Treasury office that administers and enforces economic and trade sanctions. Broker-dealers must screen customers and transactions against OFAC lists and block or report transactions when required.
Red Flags: Behaviors or indicators of potentially suspicious activity. For broker-dealers, this includes unusual trading patterns, sudden large deposits, or transfers inconsistent with a customer's stated objectives.
Politically Exposed Person (PEP): A person who has held a prominent public position (e.g., government official, senior executive of a state-owned enterprise), their immediate family, or close associates. PEP accounts often require EDD.
Structuring: The deliberate structuring of transactions below reporting thresholds to avoid detection, also known as "smurfing." Broker-dealers must monitor for patterns of such activity.
High-Risk Account: An account deemed to have a higher potential for money laundering or terrorist financing, based on the customer's profile, geography, products, or services used.
Financial Crimes Enforcement Network (FinCEN): A bureau of the U.S. Department of the Treasury that collects and analyzes information about financial transactions to combat money laundering, terrorist financing, and other financial crimes.

Ongoing Monitoring: The process of continually assessing customer activity, transactions, and account profiles to detect and report suspicious behavior in a timely manner.
Anti-Money Laundering Compliance Officer (AMLCO): The designated individual responsible for overseeing the broker-dealer's AML program, including training, reporting, and ensuring compliance with applicable laws.
Correspondent Account: An account established by a broker-dealer for a foreign financial institution to receive deposits, make payments, or handle other financial transactions. These require heightened due diligence.

DESIGNATED PERSONNEL

The Company has appointed Kimberly Miller as the **Designated AML Program Supervisor**, or "AMLCO." The AMLCO is responsible for

- Developing the Company's Anti-Money Laundering Program;
- Working with the CCO and designated Principals to implement the AML Program;
- Monitoring changes to the USA Patriot Act and other relevant AML rules and regulations, including Section 311, to ensure that the AML Program is updated as needed and new procedures are implemented;
- Acting as contact point for all employees and associated persons who have suspicions or concerns;
- Acting as the initial point of authority in the process of determining if certain unusual activities constitute reportable suspicious activities.
- Reviewing any account or other activity deemed to warrant further investigation; and
- Ensuring records related to AML are maintained in accordance with applicable rule and regulations.

The AML Chief Compliance Officer (AMLCO) will act as the central point of contact for communicating with the regulatory agencies regarding money laundering issues, unless such authority is delegated. The AMLCO will act as the final point of authority in the process of determining if certain unusual activities constitute reportable suspicious activities and ensure that the requirements under FINRA Consolidated Rule 3310 and any new, relevant rules and regulations are implemented on a continuing basis.

Also contributing to implementation and supervision of the AML policies and procedures described in this Program are the Company's designated Principals, as listed in the Written Supervisory Procedures (WSP) Manual. These Principals are charged with the daily supervision of the business activities of Registered Representatives (RRs) and will serve to receive notification from RRs and employees of unusual or suspicious activity. They will also serve to detect such activity in their daily, weekly and/or monthly reviews. These Principals may also act as a sounding board for RR suspicions and will ensure internal reporting of such suspicions to the AMLCO, when deemed necessary.

FINRA CONTACT SYSTEM

So that the Company can promptly receive alerts from FinCEN and other entities, the Company, through the FINRA Contact System, will provide the following information on each associated person designated to implement the AML Program or to receive AML-related communications, including FinCEN 314(a) notices:

- Name of AML contact person
- Mailing address
- E-mail address
- Telephone number
- Facsimile number

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 AMLCO or persons

designated to receive notices 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.

PRELIMINARY RISK ASSESSMENT

Prior to engaging in business with a new customer, Registered Representatives and their designated Principals are required to consider the following factors when opening new accounts or reviewing the activities of existing accounts:

- Whether the customer is an individual, an intermediary, public, private, domestic or foreign corporation, a financial or non-financial institution, or regulated person or entity;
- Whether the customer has been an existing customer for a significant period of time;
- How the client became a customer of the Company;
- Whether the business of the customer, or the particular type of account, is the type more likely to be involved in illicit activity (e.g., cash intensive business);
- Whether the customer'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
- Whether the customer resides in, is incorporated in or operates from a jurisdiction with bank secrecy laws, or one that has otherwise been identified by a regulatory or law enforcement agency or the Company 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 AMLCO. The AMLCO shall evaluate the facts prior to the person or entity becoming a customer of the Company and will put into place 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 customer 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 account documentation and approval process, and may be useful in the future monitoring of new accounts, if approved and opened.

Risk Factors

The following are risk factors identified by OFAC that may warrant a heightened level of scrutiny:

International transactions, including wire transfers

- High number of international transactions, cross-border transactions, or investments in a foreign investment fund or on a foreign exchange (since LFF conducts business primarily with Mexican Nationals, a high number of cross-border transactions does not in itself warrant a heightened level of security);
- Presence of overseas branches or multiple correspondent accounts with foreign financial institutions, including correspondent accounts subject to enhanced due diligence under Section 312 of the USA PATRIOT Act.

Foreign customers/accounts

A large, fluctuating client base across a number of foreign jurisdictions involving a large number of security transactions;

- Customers located in or have accounts in high-risk jurisdictions, such as countries found to be of "primary money laundering concern" pursuant to Section 311 of the USA PATRIOT Act;
- Customers located in or have accounts in countries that are havens for money laundering or are inadequately regulated, including countries identified by the Financial Action Task Force as maintaining an inadequate AML/CFT regime;
- Customers located in or have accounts in countries where local laws, regulations, or provisions (such as privacy laws) prevent or limit the collection of client identification information;
- Customers located in an offshore financial center as identified by the U.S. Department of State;
- Accounts for senior political or government officials ("politically exposed persons") of a foreign government;
- Accounts of closely held corporations;
- Accounts for unregistered or unregulated investment vehicles;
- Accounts maintained at an offshore bank.

Foreign broker-dealers who are not subject to OFAC regulations:

- Lack of information regarding beneficial owners of securities; and
- Foreign broker-dealers that act as introducing brokers.

Risks of Investments in Foreign Securities:

Practical exposure increases when investing in a foreign investment fund or foreign exchange, because of the risk that the securities are issued by a sanctioned country or party or otherwise in violation of OFAC sanctions, *e.g.,* securities of an issuer that provides financing for a sanctions target. Other risk factors include:

- Cross-border settlements involving the interaction of different settlement systems and laws in different countries;
- Foreign securities that may be more prone to misidentification in the course of a trade, *e.g.,* similar names between two foreign issuers;
- Foreign companies that issue shares in bearer form.

Personal Investment Corporations or Personal Holding Companies

- Beneficial ownership by a non-U.S. person that maintains a private banking account with a U.S. financial institution.

Very High Net Worth Institutional Accounts

- Hedge Funds
- Funds of Hedge Funds
- Other Alternative Investment Funds (Private Equity, Venture Capital Funds)
- Intermediary Relationships:
- Lack of transparency regarding securities/investments and beneficial owners;
- U.S. hedge fund with an offshore related fund where beneficial owners are offshore investors; and
- Subscription funds that originate from or are routed through an account maintained at an offshore bank, or a bank organized or chartered in an inadequately supervised and poorly regulated jurisdiction, or a foreign shell bank.

Omnibus Accounts/Use of Intermediaries:

- Potential for the use of code names to invest funds in the United States on behalf of sanctions targets, concealing the identities of the beneficial owners;
- Accounts for intermediaries held in street name that trade on behalf of third parties, such as other broker-dealers, banks, and mutual funds; and
- Cross-border trades executed for unregulated investment vehicles, *e.g.,* hedge funds, private equity funds, and other private pools of capital.

Financial Intermediaries as Customers vs Beneficial Owners

Financial institutions (such as banks, clearing firms, investment advisers, *etc.*) act as intermediaries opening accounts including master and omnibus accounts. The SEC has stated that the underlying beneficial owners are **not** "customers" subject to CIP requirements under the following circumstances outlined in the SEC's guidance:

- the omnibus account or relationship is established by or on behalf of a financial intermediary for the purpose of executing transactions that will clear or settle at another financial institution, or the omnibus account holder provides limited information to LFF solely for the purpose of delivering assets to the custody account of the beneficial owner at another financial institution;
- the limited information given to LFF about the beneficial owner is used primarily to assist the financial intermediary with recordkeeping or to establish sub-accounts that hold positions for a limited duration to facilitate the transfer of assets to another financial institution;
- all transactions in the omnibus account or sub-accounts at LFF are initiated by the financial intermediary; and
- the beneficial owner has no direct control over the omnibus account or sub-accounts at the broker-dealer.

LFF is not obligated to look through the intermediary financial institution to the underlying beneficial owners if the intermediary identifies itself as the accountholder. Even if LFF has some information about beneficial owners, the intermediary (not the beneficial owner) is treated as the customer for purposes of the CIP rule under these circumstances.
owners, the intermediary (not the beneficial owner) is treated as the customer for purposes of the CIP rule under these circumstances.

Third-Party Introduced Business

- Business introduced by an overseas bank, affiliate, or other investor based in high risk or inadequately regulated countries.

Confidential Accounts

- Private banking accounts established or maintained for non-U.S. persons or services, including financial and related services, to wealthy clients who use offshore accounts for tax avoidance purposes.

CUSTOMER IDENTIFICATION PROGRAM

Level Four Financial, LLC endeavors 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.

This Anti-Money Laundering Compliance Program does not reiterate but, rather, incorporates by reference Level Four Financial, LLC'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. 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 customers. 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 as well as FinCEN's Customer Due Diligence Rule.

Definitions. In the context of this CIP, **"customer"** (or "client" as used herein) refers to a person who opens a new account by entering into a relationship with the firm 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 also not 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, another recognized domestic national exchange or 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 AMLCO 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, 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. Accounts established at a clearing firm or through subscription way business with mutual funds or variable products companies are considered to be "accounts" of the broker/dealer for purposes of Section 326 of the US Patriot Act.

The Company may do business with entities excluded from the definition of "customer" for CIP purposes, as outlined above, in addition to individuals and entities not excluded from the definition of "customer." For entities excluded from the definition of "customer," the Company has verified this exclusion and a copy of the documentation reviewed will be maintained in the client file.

For those excluded entities the Company is not required to conduct a CIP review or verify the identity of these entities or their owners. The Company's procedures relative to CIP and verification of identity for individuals or entities not excluded from this definition are included in the rest of this section.

This section, while devoted to procedures at the account opening stage, serves as a reminder to Registered Representatives to attain the highest level of familiarity possible with all accounts, not only new accounts. While transactions by existing accounts will be monitored for potential suspicious activity, it is imperative that the customers themselves be 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 accounts be reviewed periodically to ensure up-to-date contact information and suitability data (RRs should reference their WSP Manuals for related details).

Customer Notification

BEFORE an account is opened or a relationship is established with a new customer, 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: Notice will be posted on the Company's website and notice will be included on the Company's account applications.

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

Important Notice: 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 and entity that opens an account.

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

Necessary Account Information

The Company requires its Representatives, prior to opening an account or establishing a relationship with a new customer, to obtain the following minimum identifying information on the customer. Registered representatives must also gather the following information on an entity's beneficial owners, if the entity not exempt from the definition of customer as outlined above or the FinCEN Due Diligence Rule, described below:

- Name of the person(s) or entity
- For an individual, a date of birth;
- An 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 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;
  - For an individual in a state address confidentiality program, the street address of the ACP sponsoring state agency, since the person in the program is treated as not having a residential address and the agency sponsoring the ACP or another state agency is considered as another contact person for these individuals, and
- An identification number, which will be:
  - For a U.S. person (individual or entity), a taxpayer ID number; or
  - For a non-US. 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.

If a customer has applied for, but has not received, a taxpayer ID number, Registered Representatives are permitted to open the account or 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, the account must be closed (unless the AMLCO or CCO extends this deadline in writing). 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 account may not be opened and the AMLCO must be notified to determine if 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 AMLCO will be notified. After reviewing the facts and circumstances, the AMLCO will determine if an existing account, if applicable, should be closed and whether the Company should report the situation to FinCEN on a FinCEN SAR. Notes regarding this review and recommendation will be maintained in the Company's AML files. If a filing is required, the AMLCO shall follow the Company's procedures related to SAR filings as included in this Manual.

Prohibited Transactions

Level Four Financial, LLC is prohibited from conducting transactions in any account on behalf of a sanctioned party or in certain blocked securities. Securities and funds may not be released, and securities transactions may not be executed. Securities and funds may be deposited to a blocked account, but no securities or funds will be released until the account is no longer subject to sanctions. Funds or securities may not be transferred to sanctioned parties.

Because transactions are prohibited, all open orders for a blocked account will be cancelled.

FINCEN CUSTOMER DUE DILIGENCE RULE ("CDD")

The CDD requires the Company to gather information on the beneficial owners and control persons of certain legal entities, to evaluate the nature and purpose of the customer's relationship with the firm and to develop risk-based procedures for ongoing monitoring of suspicious activities. The Company's procedures related to the ongoing monitoring for suspicious activities is described elsewhere in this manual.

Under the CDD, a legal entity includes a corporation, limited liability company, or other entity that is created by a filing of a public document with a Secretary of State or similar office; a general partnership; and any similar business entity formed in the United States or a foreign country.

In addition to the entities excluded from the definition of a customer under the USA Patriot Act, as described above, the CDD Rule excludes from the definition of legal entity the following:

- Any entity organized under the laws of the United States or of any US State where at least 51% of whose common stock or analogous equity interests are held by a listed entity;
- Issuers of securities registered under section 12 of the Securities Exchange Act of 1934 (SEA) or issuers required to file reports under 15(d) of that Act;
- A public accounting firm registered under section 102 of the Sarbanes-Oxley Act;
- A bank holding company, as defined in section 2 of the Bank Holding Company Act of 1956 (12 USC 1841) or savings and loan holding company, as defined in section 10(n) of the Home Owners' Loan Act (12 USC 1467a(n));
- A pooled investment vehicle operated or advised by a financial institution;
- An insurance company regulated by a US State;
- A financial market utility designated by the Financial Stability Oversight Council under Title VIII of the Dodd-Frank Wall Street Reform and Customer Protection Act of 2010;
- A foreign financial institution established in a jurisdiction where the regulator of such institution maintains beneficial ownership information regarding such institution;
- A non-U.S. governmental department, agency or political subdivision that engages only in governmental rather than commercial activities; and
- Any legal entity only to the extent that it opens a private banking account subject to 31 CFR 1010.620.

For each legal entity, not exempt from the requirements, the Company will document the evaluation of the nature and purpose of the customer's relationship with the Company in the customer's file.

In addition, the Company will gather required information related to the beneficial owners and control person(s) of non-exempt legal entities on a Certification of Beneficial Owners ("CBO" or similar form, which contains the information required under the CDD.

The information required to be recorded on the CBO form includes:

- The necessary account information, as outlined above, for each individual that owns, directly or indirectly, 25 percent or more of the equity interests of the legal entity.

  If the legal entity is owned by another entity, the Company must gather information related to the ultimate individual owners that have 25% or more ownership of the entity at the top of the ownership structure.
- If there is no beneficial owner who has 25% or more ownership the Company will retain documentation on how they determined no such owners exist and will record "None" on the CBO form.

- The necessary account information for the individual with significant responsibility for managing the legal entity, such as a CEO, CFO, COO, Managing Member, General Partner, President, Vice President, or Treasurer.

The Company will verify the identity of the individuals named on the CBO form in accordance with the procedures related to the verification of identity outlined below.

Further, the Company will conduct a search of the OFAC lists for all beneficial owners and control persons identified.

A copy of the CBO will be maintained in the customer files. In addition, the AMLCO will ensure that information related to the beneficial owners and control persons is reviewed periodically during the customer relationship and that the CBO form is updated and verification occurs when there are changes to the beneficial owners or control person at the legal entity and each time the entity opens a new account.

Verification of Identity

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

Documentary Means.

RRs must first attempt to verify customers' 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 AMLCO 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.

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

Non-Documentary Means.

In some cases, non-documentary methods of verification will be utilized. The Firm may use non-documentary methods (outlined below) 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.

Non-documentary methods of verifying identity include:

- Contacting a customer at his residence or place of business;
- 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;
- Obtaining a financial statement; and/or
- Any other reasonable means of attempting to verify the customer'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 AMLCO 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.

Lack of Customer ID Verification

When LFF cannot form a reasonable belief that it knows the true identity of a customer, LFF will not open an account.
Where inability to verify raises questions about the customer, filing a Suspicious Activity Report will be considered

Timing.

Registered Representatives must attempt to verify the identities of new customers prior to account opening. 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 AMLCO prior to opening the account, or 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 AMLCO shall document his/her review and shall advise the registered representative whether or not the account may be opened, or engagement entered into, prior to verification. The AMLCO's decision and any restrictions on the account or relationship shall be noted in the client file.

Reluctance on behalf of the potential customer may be considered suspicious and should be brought to the attention of the AMLCO so that he/she may determine whether additional action is required. Documentation related to the customer and the AMLCO's determination shall be maintained by the AMLCO in his or her potential suspicious activities file.

If the RR is unable to verify identity prior to account opening, they must notify their designated principal and AMLCO about the deficiency for review of other non-documentary means and appropriate action will be taken.

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).

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 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 the accounts, 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 creating debits to blocked accounts, although credits are authorized. Blocked SEC securities may not be paid, withdrawn, transferred (even by book transfer), endorsed, guaranteed or otherwise dealt in.

OFAC Specially Designated Nationals and Blocked Persons (SDN) lists can be reviewed 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 screen all new customers against these lists and will also screen existing customers at least annually. The AMLCO will ensure evidence of the initial review and evidence of annual reviews are retained in either the client file or a separate OFAC review file.

In addition, if the Company processes or facilitates wire transfers or payments to third parties on behalf of its customer, the third party receipt must be checked against the OFAC list and records maintained of this review.

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

During a search, if a potential match is found, internal due diligence must take place to determine that a number of similarities exist 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 a match is confirmed, the AMLCO must inform OFAC, within 10 business 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 AMLCO 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 AMLCO 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 AMLCO.

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 account is opened (or earlier, if required by another federal law or regulation or federal directive issued in connection with an applicable list), the AMLCO 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 AMLCO 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 AMLCO 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.

ENHANCED 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 customers' identities, questions may remain. These questions should be brought by the RR or his/her designated Principal to the AMLCO, 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 an account 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 non-cooperative with international Anti-Money laundering principles or procedures or having inadequate Anti-Money laundering measures. The following

are some of the sources the AMLCO 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)
- USA PATRIOT Act Section 311 Designated Financial Institutions
- 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 customer's account file, and will remain confidential. This information, if indicative of suspicious activity, will be used in internal or official reporting, and should be maintained as described below.

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

Enhanced Due Diligence for Some Foreign Banks

Enhanced due diligence is required for a correspondent account for a foreign bank that is operating:

- under an offshore license;
- under a license issued by a country that has been designated as being non-cooperative with international Anti-Money laundering principles or procedures by an intergovernmental group or organization of which the U.S. is a member and with which the U.S. concurs regarding the designation; or
- under a license issued by a country designated by the Secretary of the Treasury as warranting special measures due to money laundering concerns.

Such accounts are subject to risk-based enhanced due diligence, including the following:

- The AML Compliance Officer is responsible for identifying and monitoring such accounts.
- If the bank's shares are not publicly traded, identify the owners of the bank, and verify they do not appear on U.S. lists of restricted individuals or companies.
- Obtain and consider information about the bank's AML program to assess money laundering risk.
- Obtain information from the bank about the identity of any person with authority to direct transactions through any correspondent account that is a payable-through account and the sources and beneficial owner of funds or other assets in the payable-through account.
- Determine whether the foreign bank for which the correspondent account is established or maintained in turn maintains correspondent accounts for other foreign banks that use the foreign correspondent account established or maintained by LFF and, if so, take reasonable steps to obtain information relevant to assess and mitigate money laundering risks associated with the foreign bank's correspondent accounts for other foreign banks, including, as appropriate, the identity of those foreign banks.
- Monitor such accounts for potential money laundering, either manually or electronically depending on available information.
- Report the account, upon initial review or in the course of monitoring, if necessary.

If enhanced due diligence cannot be performed, the account will not be opened, trading will be suspended, a suspicious activity report will be filed, and/or the account will be closed.

Prohibition Against Correspondent Accounts for Foreign Shell Banks

LFF is prohibited from establishing, maintaining, administering, or managing a correspondent account in the United States for an unregulated foreign shell bank. The prohibition does not apply to a foreign shell bank that is a regulated affiliate. If an account is inadvertently opened for an unregulated foreign shell bank, the AML Compliance Officer must be notified, and the account will be immediately closed.

Foreign Bank Certification

When opening an account for a foreign bank, LFF is obligated to ensure the bank is not a foreign shell bank and must obtain information about the foreign bank's owners and an agent for service of process. The bank must complete the Foreign Bank Certification which must be submitted to the AML Compliance Officer with a copy of the new account application for review. Every three years the bank is also required to re-certify the information filed with LFF.

Special Measures

Some foreign jurisdictions, foreign financial institutions, international transactions, or types of accounts are designated to be of "primary money laundering concern" by the Secretary of the Treasury. This designation obligates LFF to take certain "special measures" against the primary money laundering concern. The Secretary of Treasury announces when an entity is a primary money laundering concern. These special measures include:

- A prohibition against opening or maintaining a correspondent account in the U.S. for or on behalf of the primary money laundering concern including at the time of announcement, review of existing account records to identify any prohibited accounts

- Notification to correspondent accountholders that the account may not be used to provide the primary money laundering concern with access to LFF [sample notification is included in Notice to Members 06-41 and may be transmitted by a one-time notice by mail, fax, or e-mail or by including the information in the next regularly occurring transmittal to the account, such as an account statement]

- Reasonable steps to identify indirect use of correspondent accounts by the primary money laundering concern by review of transaction-based records

The clearing firm is responsible for complying with special measures including notification of correspondent accounts and retaining records of compliance.

Due Diligence for Private Banking Accounts

Private banking accounts:

- include accounts established for a non-U.S. beneficial owner.
- include accounts where the beneficial owner is an individual:
  - who has a level of control over, or entitlement to, the funds in the account
  - who directly or indirectly controls, directs, or manages the account
  - for whom an account is established, maintained, or administered in the U.S.
- exclude accounts for hedge funds (and other pooled vehicles) and corporations (that are not personal investment companies ["PICs"].
- include accounts for PICs and trusts for the benefit of individual owners. Requirements for due diligence:

- Determine the identity of all nominal and beneficial owners of the private banking account.
- Determine the purpose and expected use of the account.
- Determine whether any such owner is a senior foreign political official.
- Determine the source(s) of funds deposited into the private banking account and the purpose and expected use of the account.
- Review the account activity:
  - to ensure consistency with information about the account.
  - to report suspected money laundering activity.

Factors considered in determining due diligence include:

- Is the client from a jurisdiction identified by the federal government as a jurisdiction subject to OFAC restrictions or as having weak AML controls?
- Is the customer's business cash intensive?

LFF cannot rely on foreign institutions to perform due diligence for private banking accounts, and due diligence obligations are ongoing. If appropriate due diligence cannot be performed for the account, the account will be closed.

Enhanced Scrutiny for Accounts of Senior Foreign Political Figures

Accounts for senior foreign political figures (including persons and entities defined in this section) are subject to enhanced scrutiny:

- Prior to opening, the account is referred to the AML Compliance Officer for review and approval.
- Review the account's home country vs. OFAC lists of jurisdictions of money laundering concern and blocked persons.
- If identified on an OFAC list, report the account, and close it.
- Review new account information about the account including employment history, sources of income and assets, whether the person/entity has existing accounts with LFF, length of time the RR has known the account, who referred the account, and other available information about account background of the account and how the account came to LFF.
- If there is inadequate information or due diligence procedures cannot be performed, refuse to open the account, or close an existing account.
  - File a SAR, if appropriate.
- If the account is approved for opening, determine whether ongoing review is necessary.
  - If ongoing review is appropriate, establish duplicate statements or another method for review of account activity by the AML Compliance Officer.
  - Review will include identifying patterns of securities transactions and securities/money transfers that may be indicative of money laundering activity, and report such activity if necessary and close the account.

Shell Companies

Shell companies can represent a potential money laundering risk. Most shell companies are formed for legitimate business reasons, but some have been used for illicit purposes. "Shell company" refers to non-publicly traded corporations, limited liability companies (LLCs), and trusts that typically have no physical presence (other than a mailing address) and generate little or no independent economic value. Legitimate purposes including holding stock or intangible assets of another business entity (such as subsidiary company shares) but are not engaged in active business operations or facilitating domestic and cross-border currency and asset transfers and corporate

mergers. State laws allow shell companies to obscure company structure, ownership, and activities, so there is little transparency to enable LFF to understand with whom they are dealing.

Agents that act as intermediaries or nominee incorporation services (NIS) can play a central role in creating, maintaining, and supporting shell companies. Some agents and NIS firms also provide individuals and businesses with nominee services that preserve the anonymity of underlying officers, directors, and stockholders.

Shell companies are subject to review which may include:

- Checking accounts and owners (if information is available) against OFAC restrictions (applies to all accounts)
- Obtaining information about underlying owners
- Obtaining assurances from the shell company representative that principals have been screened

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 customers' actions and attitudes throughout the process. While suspicious activity may normally occur in the course of servicing existing accounts, certain actions by a prospective customer 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 customer's identity proves unusually difficult and/or such customer 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 customer who wishes to engage in transactions that lack business sense, apparent investment strategy, or are inconsistent with the customer's stated business and/or strategy;
- A customer whose requirements are not in the normal pattern of or are inconsistent with the Company's business and which could be more easily serviced elsewhere;
- A customer, or person publicly associated with the customer, 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 LLCs;
- The customer's (if an entity) business activity apparently conflicts with the description of activity listed on the entity's formation documents;
- An institutional or intermediary customer 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 customer 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 customer's file. These observations, if determined valid, will used in internal or official reporting, described below.

USE OF THIRD PARTIES OR OTHER RESOURCES

The Company utilizes its clearing firms to assist in their CIP and verification efforts. The AMLCO, in conjunction with the CCO, will ensure that the clearing firm is performing functions as expected by periodically reviewing the services

being provided. In addition, the AMLCO, in conjunction with the CCO, will ensure that any third-party provider has adequate controls in place to protect confidential information and mitigate the risk of cyber-attacks.

Additionally, the firm utilizes SS&C/RCI to monitor accounts against the OFAC/Blocked Sanctions list as accounts are opened, annually and as the FinCEN lists are updated.

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.

The Company has entered into an agreement with Raymond James & Associates 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. The Company's reliance must meet the following criteria:

- It 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;
- The other financial institution has entered into a contract with the Company requiring it to certify annually 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;
- The other financial institution is regulated by a federal functional regulator (i.e., registered with the SEC.) and must have an AML Program in place; and
- Any such agreement should be described in writing and renewed annually.

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.

SPECIAL ACCOUNTS

The Company does not engage in business with the following:

- Confidential Accounts;
- Accounts for Marijuana-related Businesses;
- Omnibus Accounts;
- Private Banking Accounts;
- Accounts for Senior Foreign Political Figures; and
- Correspondent Accounts.

All Company employees and registered persons must report to the AMLCO any perceived attempt on behalf of a customer to open such an account with the Company.

Should such an attempt be detected, the AMLCO will investigate and follow up with actions designed to halt the activities and fulfill any and all reporting obligations.

If the Company begins engaging in business with these accounts in the future, the AMLCO will ensure the Company has adopted required procedures related to the monitoring of activities in the accounts and reporting as required.

MONITORING FOR POTENTIAL SUSPICIOUS ACTIVITY

Besides striving to "know your customer," an objective of Level Four Financial, LLC's Anti-Money laundering efforts is to identify potentially suspicious and unusual activity in its customers' accounts. Monitoring transactions is essential to determining if unusual or suspicious activities are taking place, which may be related to money laundering.

Ongoing Monitoring

Level Four Financial, LLC is currently in the practice of monitoring its business activity by conducting reviews on a periodic basis, including, at least, daily, monthly, and annual reviews. Such reviews may be either manual or automated and include, for example, trade approvals, reviews of exception reports and daily blotter reviews. 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.

Exception Reports

Currently the Company makes use of certain exception reports; these reports are described in the Company's WSP manual. The Company's procedures require periodic review of these reports by a designated Principal. In order to bolster its money laundering detection efforts, the AMLCO will review these exception reports monthly.

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, as 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.

Suspicious Activity—Possible Red Flags

Indicators of potential suspicious activities can occur at any time during the Company's relationship with the customer. While there is no definition of "unusual or suspicious," certain indicators may evidence potential money laundering or fraudulent activities. Examples of these indicators follow:

Customers – Insufficient or Suspicious Information

- 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.
- Customer with no discernible reason for using the Firm's service.

Efforts to Avoid Reporting and Recordkeeping

- Reluctant to provide information needed to file reports or fails to proceed with transaction.
- Tries to persuade an Associated Person not to file required reports or not to maintain required records.
- Unusual concern with the Firm's compliance with government reporting requirements and the Firm's AML policies and procedures.

Certain Deposits or Dispositions of Physical Certificates

- Physical certificate is titled differently than the account.
- Physical certificate does not bear a restrictive legend but, based on history of the stock and/or volume of shares trading, it should have such a legend.
- The customer's explanation of how he or she acquired the certificate does not make sense or changes.

Certain Funds Transfer Activities and Cash Deposits

- 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 engages in, or attempts to engage in, transactions involving cash over $10,000 or cash equivalents or other monetary instruments that appear to be structured 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 engages 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 Level Four Financial, LLC to be high-risk;
- A customer's account has unexplained or sudden extensive wire activity, where previously there had been little or no wire activity, without any apparent business purpose;
- A 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;
- For no apparent reason, a customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers;
- Wire activity that is unexplained, repetitive, unusually large, or shows unusual patterns with no apparent business purpose.

Activity Inconsistent with Business

- A customer engages in excessive journal entries between unrelated accounts without any apparent business purpose;
- A customer requests that a transaction be processed in such a manner so as to avoid the Company's normal documentation requirements;

- A 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 a transfer of the proceeds out of the account;
- A customer engages in transactions involving certain types of securities, such as penny stocks, Regulation "S" stocks and bearer bonds, which, although legitimate, have been utilized in connection with fraudulent schemes and money laundering activity;
- Two or more accounts trade an illiquid stock suddenly and simultaneously;
- Customer engages in prearranged or other non-competitive trading, including wash or cross trades of illiquid securities;
- Customer has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason;
- Customer transactions include a pattern of receiving stock in physical form or the incoming transfer of shares, selling the position, and wiring out proceeds;
- Customer's trading patterns suggest that he or she may have inside information.
- Transactions patterns show a sudden change inconsistent with normal activities.
- Maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
- Appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.

Transactions Involving Insurance and Variable Annuity Products

- A customer has repeated cancellations of variable annuity contracts during the look-back period;
- Cancels an insurance contract and directs funds to a third party;
- Structures withdrawals of funds following deposits of insurance annuity checks signaling an effort to avoid BSA report requirements;
- Rapidly withdraws funds shortly after a deposit of a large insurance check when the purpose of the fund withdrawal cannot be determined;
- Opens and closes accounts with one insurance company and then reopens a new account shortly thereafter with the same insurance company, each time with new ownership information;
- Purchases an insurance product with no concern for investment objective or performance;
- Purchases an insurance product with unknown or unverifiable sources of funds, such as cash, official checks, or sequentially numbered money orders.

Transactions Involving Penny Stock Companies

- Company has no business, no revenues, and no product.
- Company has experienced frequent or continuous changes in its business structure.
- Officers or insiders of the issuer are associated with multiple penny stock issuers.
- Company undergoes frequent material changes in business strategy or its line of business.
- Officers or insiders of the issuer have a history of securities violations.
- Company has not made disclosures in SEC or other regulatory filings.
- Company has been the subject of a prior trading suspension.

Other Suspicious Customer Activity

- A customer deposits bearer bonds, followed by an immediate request for the disbursement of funds;
- A customer exhibits a total lack of concern regarding risks, commissions, or other transaction costs;
- Unexplained high level of account activity with very low levels of securities transactions.
- Law enforcement subpoenas.
- Large numbers of securities transactions across a number of jurisdictions.

- Buying and selling securities with no purpose or in unusual circumstances (e.g. churning at customer's request).

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

Othe Requests to Monitor Accounts

Regulators or law enforcement agencies may ask the industry's cooperation in identifying accounts for individuals or entities under investigation or suspected of criminal activities.
The Chief Compliance Officer is responsible for responding to such requests; providing the necessary information; and retaining records of requests, reviews conducted pursuant to requests, and information provided to authorities.

Specific Activity Monitoring

Certain activities require additional monitoring and possible reporting to detect potential suspicious activities. The Company has adopted the following procedures related to the activities:

Wire Transfers

Wire transfer approval and execution compliance procedures are described in the Company's WSP Manual and must be followed. Verification of customer identification must be conducted in accordance with the Company's established practices (or those of its clearing firm, if applicable). Further the Company must maintain records as outlined in the "Travel Rule."

The "Travel Rule" arises under the Treasury Department regulations issued by FinCEN pursuant to the 1996 amendments to the Bank Secrecy Act. Where the Company is transmitting funds equal to or greater than US$3,000 (or its foreign equivalent), it must 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

Back-office personnel are required to keep a log of wire transfer activity, reports from the clearing firm, and copies of customer wire requests. The documentation must record customers' names and the dates, dollar amounts and geographic destinations of wire transfers. The wire information will be reviewed at least monthly by the AMLCO in order to detect patterns of unusual behavior, such as recurring dollar thresholds, increased or aberrant volume, or high-risk destinations. In his or her review of wire transfers, the AMLCO will also confirm that proper record keeping under the "Travel Rule" is conducted. Evidence of the AMLCO's review shall include his/her initials, the date of review and any notes recorded on the wire documentation reviewed.

Foreign Currency Transactions

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 AMLCO should be notified.

Receipt of Security Certificates

The Company currently accepts securities certificates from customers and records them on the Securities Received and Delivered blotter. The AMLCO will review this blotter at least monthly in order to detect potential structuring of such deposits and evidence his/her review by initialing and dating the blotter.

If the Company receives low-priced or foreign securities the AMLCO, in conjunction with the CCO and other Principals and/or the clearing firm if applicable, will review the certificates and issuers to ensure that these certificates are legitimate and that they can be accepted for deposit.

Transfer of Fund or Securities to Third Parties

The procedures related to the transfer of customer funds and securities either among accounts or to external recipients are describe in the Company's WSP Manual and must be followed. Verification of the receipt's identity and OFAC checks must be completed in accordance with the Company's established practices (or those of its clearing firm, if applicable).

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

The AMLCO 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.

Monitoring by Clearing Firm(s)

LFF will work with the clearing firms to exchange information, records, data, and exception reports as necessary to comply with AML laws. Required certifications for information sharing are on file. As a general matter, the clearing firm will monitor LFF's customer activity on LFF's behalf, and the clearing firm will be provided with proper customer identification information as required to successfully monitor customer transactions. LFF's and the clearing firm's responsibilities are included in the clearing agreement and each firm is responsible for its own independent compliance with AML laws. LFF and the clearing firm cannot disclaim their respective responsibilities to comply with AML requirements.

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.

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 AMLCO.) 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 document the suspicious activity, including the steps they have taken to review the activity, and immediately report the activity to the AMLCO.

In certain situations, the AMLCO should notify CCO and immediately contact federal law enforcement by telephone. Examples of such emergency situations include:

- A customer is listed on the OFAC list;
- A customer's legal or beneficial account owner is listed on the OFAC list;
- A customer 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 customers, is not required to also file a FinCEN SAR with FinCEN. OFAC will report the filed information to FinCEN. However, if suspicions exist beyond the details provided in the field OFAC report, the Company must file a separate FinCEN SAR with FinCEN to report those suspicions.

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 owner 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 customer's account documentation in an effort to better know the customer, has recorded certain notes in the customer'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 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, described below under "Reporting Procedures—Internal."

Note that RRs and all employees may have suspicions at any stage of their involvement with customers. 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 customer 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.

Reporting Procedures

To avoid unsubstantiated (and embarrassing) official reporting any potential suspicious activities must be reported, all such activities must be reported to the AMLCO for review in writing. The AMLCO will review the details related to the suspicious activity and will then recommend any of the following:

- dismissal of the suspicion;
- 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 AMLCO will implement such monitoring and track the results in order to later decide whether to dismiss or officially report the suspicious activity.

If immediate official reporting is warranted, the AMLCO will conduct such reporting, as described below.

In the event an employee suspects violations committed by the AMLCO, the employee must report such suspicion directly to the CCO. Such reports will be confidential and will result in no retaliation to the employee.

Section 356 of the USA PATRIOT Act requires ALL broker-dealers to file **Suspicious Activity Reports by the Securities and Futures Industry (**FinCEN SAR). The U.S. Department of the 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 AMLCO, once having determined that a FinCEN SAR filing is required, will complete and file the form with FinCEN within 30 days of being aware of the suspicious transaction(s). An additional 30 days to file is allowed when the person is unknown. Reporting must be done electronically and requirements for filing can be found in FinCEN's website (www.fincen.gov).

The Company is not required to close accounts (i.e., cease doing business with clients) that are the subject of a filed FinCEN SAR. 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 six 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.

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 AMLCO shall be responsible for maintaining all SAR related filings and supporting documentation.

Compromised Accounts

If an unauthorized person may have gained entry or attempted entry to a customer's account, the AML Compliance Officer and the Chief Compliance Officer will take the following actions, depending on the nature and scope of the intrusion.

- Monitor, limit, or temporarily suspend activity in the account
- Contact the customer using CIP information on file for him/her, describe what has been found, and verify that there has been an attempted or actual identity theft
- Determine if there is a heightened risk of ease of access such as a customer's lost wallet, mail theft, a data security incident, or the customer gave account information to an imposter claiming to represent LFF or the customer gave information to a fraudulent web site
- Check similar accounts where there may be unauthorized access
- Collect incident information including (if available):
  - Firm information (both introducing and clearing firms: firm name, CRD number, contact name and telephone number)
  - Dates and times of activity
  - Securities involved (name and symbol)
  - Details of trades or unexecuted orders
  - Details of wire transfer activity
  - Customer accounts affected by the activity including name and account number
  - Whether the customer will be reimbursed and by whom
- Alert other appropriate firm personnel to be aware of unusual activity in other customer accounts and notify the AML Compliance Officer of any such incidences
- Identify, to the extent possible, the cause of the account intrusion (i.e., the firm's system was compromised; individual account was hacked); whether the customer has been subject to identity theft; whether intrusion is limited to one account or whether it involves multiple accounts
- Notify clearing firm, if applicable
- Contact the SEC, FINRA, and state regulators
- If appropriate, contact law enforcement such as the FBI or the U.S. Postal Inspector, if mail is involved
- Determine whether LFF must provide a specific type of notification to the customer or others under state law
- Determine whether a SAR should be filed
- Review LFF's insurance policy which may require timely notice or prior consent for any settlement
- Provide customer assistance to minimize the impact of potential or actual identity theft, as applicable and determined by the AML Compliance Officer:

  - Consider changing passwords, security codes or other ways to access threatened accounts
  - Offer to close the account and reopen with a new account number
  - Consider not collecting on the account or selling it to a debt collector
  - Advise the customer to go to the FTC Identity Theft Web Site (http://www.ftc.gov/bcp/edu/microsites/idtheft); calling the FTC's Identity Theft Hotline (877-438- 4338); or writing the Identity Theft Clearinghouse (FTC, 6000 Pennsylvania Avenue, NW, Washington, D.C. 20580)

CURRENCY AND MONETARY INSTRUMENT TRANSPORTATION REPORT

Pursuant to SEC Rule 17(a)-8, it is the policy of Level Four Financial, LLC 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) within 15 days of the receipt of the currency or monetary instrument. 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 AMLCO 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.

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 AMLCO should be notified.

Cash Equivalents

The Company currently accepts cash equivalents, including cashier's checks, money orders and traveler's checks and records them on the Checks Received and Delivered blotter. The AMLCO will review this blotter at least monthly in order detect potential structuring of such deposits and evidence his/her review by initialing and dating the blotter.

Transactions Involving Currency over $10,000

The Bank Secrecy Act requires the Company to file currency transaction reports (CTR or FinCEN Form 104) in accordance with U.S. Treasury Department regulations. If LFF accepts a currency deposit exceeding $10,000, it is required to electronically file a Currency Transaction Report (CTR, Form 112) with the Financial Crimes Enforcement Network (FinCEN). Multiple transactions by the same person equaling over $10,000 in any one day must also be reported.
"Currency" is defined as the coin and paper money of the U.S. or legal tender of other countries. Currency also includes U.S. silver certificates, U.S. notes, federal reserve notes, and official foreign bank notes customarily used and accepted as a medium of exchange in a foreign country. CTRs must be filed by the 15th calendar day after the day of the transaction and kept for 5 years.

Transactions Involving Currency Under $10,000

IRS Publication 1544 defines "Cash" as a cashier's check, bank draft, traveler's check, or money order you receive, if it has a face amount of $10,000 or less, ***AND*** you receive it in: (a) A "designated reporting transaction," or (b) Any transaction in which you know the payer is trying to avoid the reporting of the transaction on Form 8300.

Also, a cashier's check, bank draft, traveler's check, or money order with a face amount of more than $10,000 is not treated as cash. These items are not defined as cash and you do not have to file Form 8300 when you receive them because, if they were bought with currency, the bank or other financial institution that issued them must file a report on FinCEN Report 112.

Designated Reporting Transaction

A designated reporting transaction is the retail sale of any of the following:

A **consumer durable**, such as an automobile or boat. A consumer durable is property, other than land or buildings, that:

- Is suitable for personal use,
- Can reasonably be expected to last at least 1 year under ordinary use,
- Has a sales price of more than $10,000, and
- Can be seen or touched (tangible property).

For example, a $20,000 car is a consumer durable, but a $20,000 dump truck or factory machine is not. The car is a consumer durable even if you sell it to a buyer who will use it in a business.

1. A **collectible** (for example, a work of art, rug, antique, metal, gem, stamp, or coin).

2. **Travel or entertainment**, if the total sales price of all items sold for the same trip or entertainment event in one transaction (or related transaction) is more than $10,000.

Transactions Involving Currency or Bearer Instruments Over $10,000 Transferred Into Or Outside the U.S.

Broker-dealers are required to file a Currency and Monetary Instrument Transportation Report (CMIR, Form 105) with the U.S. Customs Service to report transactions in currency and/or bearer instruments which alone or in combination exceed $10,000 and which are shipped or transported into or outside the U.S. This filing is not required for currency or other monetary instruments mailed or shipped through the postal service or by common carrier. LFF (or its clearing firm) is responsible for filing these reports and maintaining records of them. CMIRs must be filed within 15 days after the receipt of the currency or monetary instruments.

State Reporting Requirements

States have adopted various currency and suspicious activity reporting requirements. Most states have entered into an agreement with FinCEN to provide them with duplicate copies of forms filed by broker-dealers. Some states, however, require duplicate filing with the states themselves at the time the broker-dealer files with a federal agency. LFF will file reports as required under state requirements.

OFAC or SEC REPORTING

Should a customer be identified as an entity listed on current OFAC lists or the SEC Control List, the AMLCO 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.

Blocking Property and Disbursements

Any blocked account will not be permitted to engage in transactions other than the acceptance of deposits of funds or securities. Open orders of blocked accounts will be cancelled. Disbursements of funds or securities may not be

made to sanctioned parties. Both LFF and the clearing firm are responsible for monitoring requests for disbursements.

Reporting Blocked Property and Legal Actions

When an account or disbursement is blocked or a blocked security is identified, OFAC will be notified within 10 days of blocking. If LFF blocks an account or security, it will file the necessary report with OFAC. Reports filed by LFF will be retained in a file of blocked accounts or securities. Information to be reported includes:'

- Owner or account party
- Property and property location
- Existing or new account number
- Actual or estimated value
- Date property was blocked
- Copy of the payment or transfer instructions
- Confirmation that funds have been deposited in a blocked account that is identified as blocked
- Name and phone number of contact person at LFF

For rejected disbursements, the following information is to be filed:

- Name and address of the transferee financial institution
- Date and amount of the transfer
- Copy of the payment or transfer instructions
- Basis for rejection
- Name and phone number of contact person at LFF

Legal Actions Involving Blocked Property

U.S. persons involved in litigation, arbitration, or other binding alternative dispute resolution proceedings regarding blocked property must provide notice to OFAC. Copies of all documents associated with the proceedings will be submitted by Compliance to the OFAC Chief Counsel at the U.S. Treasury Department within 10 days of their filing. In addition, information about the scheduling of any hearing or status conference will be faxed to the Chief Counsel.

FOREIGN BANK AND FINANCIAL ACCOUNTS REPORTS (FBAR)

Certain "United States persons" that maintain accounts (including any account where the person has a financial interest in, or signature or other authority over) in foreign jurisdictions and with aggregate balances exceeding $10,000 are required to electronically file the **Foreign Bank Account Report (FBAR)** Form 114 with FinCEN on or before June 30th of each calendar year for accounts maintained during the previous calendar year. The AML Compliance Officer is responsible for filing the annual report if it is required for LFF.

The filing requirement applies to:

- Non-resident aliens and foreign entities "in and doing business" in the U.S.
- All forms of U.S. business entities, trusts, estates with foreign accounts.
- U.S. citizens and residents with signature or other authority over a foreign account.
- Trust beneficiaries with a greater than 50% beneficial interest in a trust with a foreign account.
- U.S. citizens and resident stockholders with greater than 50% of the value or vote of the shares of a corporation with foreign accounts.

- Entities that are disregarded for tax purposes, such as limited liability companies.

The filing requirement does not apply to certain entities or situations. The regulation should be consulted for specific exemptions or conditions of exemptions.

- If the account is maintained in the United States, it is not considered a foreign account even if it holds foreign assets.
- An omnibus account held by a custody bank that holds assets both in the U.S. and outside the U.S. is not considered a foreign account unless the customer has direct access to its foreign holdings maintained at the foreign institution.
- Certain entities are excluded including: foreign hedge funds, venture capital funds, or private equity funds; tax-exempt investors that own offshore "blocker corporations;" government pension funds; pension plan participants and IRA owners (provided the trustee files a FBAR); investment advisers and employees of such advisers that provide advice to SEC-registered entities; remainder interests in trusts and beneficiaries of discretionary trusts; employees of a U.S. or foreign entity that issued a class of foreign equity (including ADRs) registered with the SEC.

There also are exemptions for officers or employees with signature or other authority over certain foreign financial accounts but no financial interest in the reportable account. The regulation should be consulted for details regarding who is not required to notify FinCEN regarding signature or other authority over such an account.
LFF does not have financial interest in, signature authority or other authority over any bank account, securities account, or other financial account that the firm has in a foreign country in which the aggregate value exceeds $10,000. Therefore, the above policy pertaining to Foreign Bank Account Report is for informational purposes only.

State Reporting.

Certain states require reporting to a state authority. The AMLCO, upon filing official forms with federal authorities, should make efforts to determine respective obligations of the state where the Company is domiciled.

Clearing Firm Reporting

Consistent with Rule 3230, the Company's agreement with its clearing firm must delineate responsibilities, including those relating to money laundering prevention. While it is clear from the scope of this Program that the Company intends to fulfill its obligations without solely relying on its clearing firm, the Company has delegated certain reporting requirements to its clearing firm. The Company's clearing firm, Raymond James & Associates, has agreed to conduct the annual OFAC screening on the company's behalf.

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 FinCEN SAR, 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 FinCEN SARs, 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 FinCEN SARs and their accompanying documentation for at least five years and will keep other documents according to existing Bank Secrecy Act and other record keeping requirements, including certain SEC rules that require six-year retention.

The Company shall maintain these reports for a period of no less than five years (see above for requirements on CIP information). All FinCEN SAR's filed with authorities must be maintained in the confidential records of the AMLCO, separate from the other books and records of the Company. The AMLCO is responsible for ensuring compliance with these record keeping policies.

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 FinCEN SAR. 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 FinCEN SAR'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 filed 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 AMLCO will ensure that this AML Program is amended to include procedures on sharing SARs with parent entities.

In the event the Company receives a subpoena requesting a FinCEN SAR or related information, the request should be forwarded immediately to the AMLCO. The AMLCO 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 a FinCEN SAR 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. In The AMLCO will file with FinCEN an initial 314(b) certification before any sharing occurs and annually on the anniversary of the previous filing. The certification is now completed using the same system as is reviewed for 314a notification and a reminder is posted annually when a renewal is required. Once a firm has filed this certification, it can access the names of other institutions with whom it is acceptable to share information.

In most cases a 314(b) notification is only required when a firm knows it will be sharing information with another entity. However, the Company has a clearing arrangement with Raymond James and Associates, and the clearing

agreement requires that the Company file a 314(b) certification annually so that information can be shared with or by its clearing firm about particular suspicious transactions or so a copy of the FinCEN SAR may be shared with or by its clearing firm. The AMLCO shall ensure that the 314(b) certification is filed upon entering into the clearing agreement and annually thereafter. The Company will not share a FinCEN SAR, if the subject of the FinCEN SAR is the clearing firm itself, or one of its employees.

A copy of the 314(b) confirmation letter from FinCEN shall be maintained in the Company's Information Sharing or 314(b) file as evidence that the required filing has been made.

Response to FinCEN requests

The AMLCO is designated to respond to all requests made by FinCEN relating to money laundering or terrorist activity. The AMLCO 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, the AMLCO 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, or longer if specified in the notice, to determine if any current or prior clients 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 AMLCO shall review all available information to confirm the match. If the AMLCO determines the match to be confirms, the AMLCO within two weeks or by the date set forth in the notice, must disclose to FinCEN that it has a match. The requesting law enforcement agency will then follow-up directly with the Company. The AMLCO 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 utilize a FinCEN review log showing the date of the notice, reviewer's name and date of review. If the firm retains a printed copy of the list, the AMLCO must ensure that list is kept is a secure location and access is granted only to persons who would have access to the electronic list due to the confidential nature of the lists and their limited applicability.

Should the Company receive requests from other enforcement authorities, the AMLCO 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 seven days after receipt of the request. The AMLCO will ensure that, within 10 days, the Company will close any account for a bank—that it learns about from the Department of the Treasury or the Department of Justice—that has failed to comply with a summons or has contested a summons The AMLCO 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 AMLCO 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.

Requests by Law Enforcement to Maintain Accounts

Law enforcement agencies may have an interest in having accounts remain open despite suspicious or potential criminal activity in connection with the account. The AML Compliance Officer will consider such requests and, if the account will remain open, require the federal law enforcement agency to provide a written request issued by a supervisory agent or by an attorney within the U.S. Attorney's Office or another office of the Department of Justice. If requested by a state or local law enforcement agency, the letter must be issued by a supervisor or local prosecutor's office.

The written request must include:

- the agency's request that the account remain open;
- the purpose of the request; and
- the duration of the request (not to exceed 6 months). The request will be retained for 5 years.

If LFF is aware the account is under investigation (because of a subpoena, 314[a] request, National Security Letter, or similar communication), the requesting law enforcement agency will be advised before making a decision about the status of the account.

National Security Letters

National Security Letters (NSLs) are written investigative demands that may be issued by the local Federal Bureau of Investigation and other federal government authorities conducting counterintelligence and counterterrorism investigations to obtain, among other things, financial records of broker-dealers. **NSLs are highly confidential. LFF and its employees are barred from disclosing to any person that a government authority or the FBI has sought or obtained access to records.**

The AML Compliance Officer is responsible for responding to an NSL and maintaining the confidentiality of the letter and the response. If an SAR-SF is filed after receiving an NSL, the SAR-SF cannot refer to the receipt or existence of an NSL. The SAR-SF will only contain detailed information about the facts and circumstances of the detected suspicious activity.

Grand Jury Subpoenas

The receipt of a grand jury subpoena concerning a customer does not in itself require the filing of a Suspicious Activity Report (SAR-SF). When a grand jury subpoena is received, the AML Compliance Officer will:

- Conduct a risk assessment of the customer subject to the subpoena as well as review the customer's account activity.

- If suspicious activity is identified during the risk assessment and review, the risk assessment will be elevated, and a SAR-SF will be filed. The SAR-SF will not contain any reference to the receipt or existence of the subpoena. The SAR-SF will only contain detailed information about the facts and circumstances of the detected suspicious activity.

The existence of a subpoena and any response are confidential and may not be disclosed directly or indirectly to the person who is the subject of the subpoena. The AML Compliance Officer will maintain the subpoena and any response in a confidential file and will only share information with those authorized.

Foreign Bank Correspondent Accounts

Upon receipt of a written request from a Federal law enforcement officer for information about a foreign bank correspondent account, the AML Compliance Officer will provide the requested information no later than 7 days after receipt of the request.

Compliance will terminate any correspondent relationship with a foreign bank within 10 business days of receiving a notice from the Treasury Dept. or the U.S. Attorney General that the foreign bank failed either to comply with a summons or subpoena or to contest it in a U.S. court.

INDEPENDENT TESTING

Frequency of Testing.

The Company's AML Program will be tested as described below once 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;
- Review of forms filed with authorities;
- 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 AMLCO's records as they relate to specific monitoring of transactions or accounts, 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 will convey the results of his or her review in the testing report. The AMLCO must present all reports to a member of senior management 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 AMLCO shall ensure that corrective action 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 has appointed an outside service provider to conduct periodic testing of its AML Program. The CCO or AMLCO has reviewed this party's qualifications and has determined that he or she is qualified to conduct testing as required under FINRA Consolidated Rule 3310. The information reviewed in evaluating the provider's

qualification and a copy of the contract/engagement agreement for the test are retained in the Company's AML testing file for the applicable year of the test.

EMPLOYEE TRAINING

Level Four Financial, LLC 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 AMLCO to provide AML training to supervisory and registered personnel. Certain employees may require additional specific training if their roles merit it (for instance, cashiering, margin or other operations personnel) and the AMLCO will coordinate such additional training, when necessary.

Training will be provided annually, or more frequently when deemed appropriate by the AMLCO. The AML training will be based on the Company's business and address areas related to AML relative to the company and its business. Training is provided as part of the Company's Firm Element Training.

The Company's training program 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 AMLCO 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 AMLCO for review and retention.