SPIRE INVESTMENT PARTNERS, LLC

CUSTOMER IDENTIFICATION PROGRAM ("CIP")

Under Section 326 of the USA PATRIOT Act, "customer" is defined as the account holder. The person or entity that opens a new account is the customer to which all of the CIP criteria must apply. Excluded from the definition of customer are (a) financial institutions regulated by a federal regulator, (b) banks regulated by a state (including credit unions, private banks and trust companies), (c) federal, state and local government entities and (d) corporations whose shares are publicly traded on U.S. exchanges.

Under Section 326 of the USA PATRIOT Act, "account" is generally defined as a formal or contractual relationship with the broker-dealer or Investment Advisor to provide financial products and/or services. Excluded from this definition are (a) accounts acquired via acquisition, merger, purchase of assets or assumption of liabilities and (b) accounts opened for the purpose of participating in an employee benefit plan under the Employee Retirement Income Security Act (ERISA).

PROCEDURES

We have established new account opening procedures which require our associated personnel to collect and use information on the account holder's identity, employment, wealth, net worth, and sources of income to detect and deter possible money laundering and terrorist financing.

Section 326 of The USA PATRIOT Act does not require that we look through a trust or similar account to its beneficiaries, or with respect to an omnibus account established by an intermediary, if the intermediary is identified as the account holder. Furthermore, we do not have to verify the identity of those who have trading authority over an account.

Prior to opening an account, we must minimally obtain:

- A name
- Date of Birth
- An address
  - For an individual, a residential or business street address
  - For an individual who does not have a residential or business

street address, an APO or FPO box number or business street address of a next of kin or other contact individual would be required.
- For other than an individual (corporation, partnership, trust, etc.), a principal place of business, local office or other physical location

- An identification number
  - For a US person, a taxpayer identification number (Social Security Number)
  - For a non-US person, one or more of the following:
    - A taxpayer identification number
    - A passport number and country of issuance
    - An alien identification card number
    - The number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard

We will verify the information within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering or terrorist financing activity, we will, after internal consultation with the firm's AML Principal, file a Suspicious Activity Report-SF ("SAR-SF") in accordance with applicable law and regulation.

Given proof that a natural or non-natural customer has applied for, but has not yet received, a taxpayer identification number, our CIP program allows the account to be opened, so long as an appropriate Principal has approved the account in all other aspects. Our policy is that all such accounts are to be closed within 30 days if the taxpayer identification number has not yet been received. Exceptions to this policy may only be made if approved (such approval documented by initials and date on the new account form) by a Principal. In addition, a note must be made to the file (signed by a Principal) indicating (a) why such an extension was granted and (b) the period of time for which the extension is in place. At the point when the exception time limit has been reached, the same procedures must be adhered to as in the first instance of allowing such an account to be opened.

DOCUMENTARY VERIFICATION

Individual

- unexpired government-issued ID evidencing nationality and residence and bearing a photograph or similar safeguard (driver's license, passport, etc.)
- other documents as may be required by our policies and procedures that allow us to establish a reasonable belief that it knows the true identity of the customer

Non-Individual

- documents showing the existence of the entity, such as certified Articles of Incorporation, government-issued business license, Partnership Agreement, trust instrument, etc.

NON-DOCUMENTARY VERIFICATION

When it is not possible to examine original documents, every effort should be made to use a variety of identification verification methods. Where documents (such as government issued IDs) are utilized to identify a customer, we are not required to take steps to determine the validity of the document; we may rely on the document itself as verification of identity.

A further reason why relying solely on documented identification may not be sufficient is the fact that, in cases of outright fraud, the perpetrator is likely to have seemingly valid identification documents, either through identity theft or through illegally obtained documents.

Therefore, except in the most obvious of low-risk instances, supervising principals at the time of the account opening, upon review, may require some non-documented verification to back up the documented verification.

Methods:

- Use the non-documentary verification facilities of our clearing firm.
- 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. (Compare information obtained from the customer against databases, such as Equifax, Experion, Lexis/Nexis, or other in-house or custom databases.) - or Online whitepages.

- Compare information obtained from customer with information available from a trusted third-party source (such as a credit report)
- Checking references with other financial institutions
- Obtaining a financial statement
- An analysis of the logical consistency between information supplied (such as name, street address, zip code, telephone number, date of birth and SS#). For instance, does the zip code match the city/state, is the area code given appropriate for the address, does date of birth seem too recent for the individual's appearance, etc.?

We will always use non-documentary methods of verification in the following situations:

(1) when the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;
(2) when the firm is unfamiliar with the documents the customer presents for identification verification;
(3) when the customer and firm do not have face-to-face contact; and
(4) when there are other circumstances that increase the risk that the firm will be unable to verify the true identity of the customer through documentary means.

RISK-BASED IDENTITY VERIFICATION REQUIREMENTS

Due to our commitment to having an effective AML Program, our AML Principal, in conjunction with other senior management and compliance personnel, has created a risk-based customer verification program.

While we believe that we will be able to verify the majority of our customers adequately through documentary and non-documentary means and by adhering to the minimal requirements set forth in The USA PATRIOT Act, there will be instances where the risk of not knowing the customer sufficiently may be heightened for certain accounts.

For certain customers identified as having heightened risk, we require that the identification go beyond the customer. Beneficial owners, control individuals, individuals given trading authority, etc. may require identification in certain instances.

Type of accounts which will fall under a more involved verification process include, but are not necessarily limited to:

- Corporations, trusts, partnerships created in a jurisdiction that have been designated by the US as a primary money laundering haven, or that have been designated as non-cooperative by an international body.
- Corporations, trusts, partnerships conducting a substantial business in a jurisdiction that have been designated by the US as a primary money laundering haven, or have been designated as non-cooperative by an international body.
- For the above, we require that information be obtained about individuals with authority or control over such accounts.

Additional Inquiries: In creating this AML CIP, we acknowledge our obligations under suitability and fair dealing requirements to collect customer identification information. Depending on the nature of the account, supervising principals, under the guidance of our AML Principal, will take the following additional steps, to the extent reasonable and practicable, when we open an account:

- Inquire about the source of the customer's assets and income so we can determine if the inflow and outflow of money and securities is consistent with the customer's financial status.
- Gain an understanding of what the customer's likely trading patterns will be, so that any deviations from the patterns can be detected at a later date.

Individuals responsible for final approval of new accounts will be given sufficient training so as to be able to identify additional accounts which may also require more than the minimal customer identification verification requirements.

In addition to the information that we are required to collect under various FINRA and SEC rules, we must also establish, document and maintain a CIP for anti-money laundering purposes.

Our AML Principal is responsible for ensuring that our CIP program has in place reasonable written procedures to:

- collect minimum customer identification information from each customer who opens an account;
- utilize risk-based measures to verify the identity of each customer who opens an account;
- record customer identification information and the verification methods and results;
- provide notice to customers that we will seek identification of information; and,
- compare customer identification information with government-provided lists of suspected terrorists.

In addition, our AML Principal, in partnership with senior management, will ensure that we have an appropriate training program for all associated personnel, which fully explains what is required of them when opening a new account and in general what they must know about our AML Program and the laws which govern it.

Supervising Principals are responsible for reviewing all account opening documentation gathered by the registered representative PRIOR to opening the account. These reviews will include checking against a list of the types of information required for each type of account and documenting why any account is opened absent that information. All review activities, including the results of OFAC and other lists checked, will be retained in client files, along with information concerning any questions which were raised and satisfactorily answered during the review process.

If OFAC and other checks are undertaken by a third party on our behalf, our registered personnel will not be required to do these checks, but our AML Principal is responsible for ensuring that they are accomplished and that we receive proof of such efforts on our behalf to retain in the files.

Our AML Principal will ensure that our verification is documented, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancy in the identifying information. We will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. We will maintain records of all identification information for five years after the account has been closed; we will retain records made about verification of the customer's identity for five years after the record is made.