Spire Investment Partners

AML Manual

March 2023

Table of Contents

Overview 4

Compliance Officer Contact Information 5

Compliance Officer Designation and Duties 6

Emergency Telephone Notification to the Government 7

Giving Information to Federal Law Enforcement Agencies and Other Financial Institutions 8

National Security Letters (NSLs) 9

Grand Jury Subpoenas 10

Sharing Information with Other Financial Institutions 11

Checking of OFAC and Other Government Lists 13

Customer Identification Program (CIP) 14

Customer Notification 19

Closing Account after Failure to Verify Customer Identity 21

Customers Who Refuse to Provide Information 22

Freezing of Accounts 23

Reliance on Another Financial Institution 24

Customer Due Diligence 25

Foreign Correspondent Accounts and Foreign Shell Banks 28

Private Banking Accounts/Senior Foreign Political Figures 29

Additional Areas of Risk 30

Monitoring Accounts for Suspicious Activity 31

Red Flags 33

Filing a Suspicious Activity Report (SAR) 36

Suspicious Transactions and Bank Secrecy Act (BSA) Reporting 41

Bank Secrecy Regulations - Special Measures 42

High Risk and Non-Cooperative Jurisdictions 43

Currency Transaction Reports (CTRs) 44

Currency and Monetary Instrument Transportation Reports (CMIRs) 45

Recordkeeping 46

Suspicious Activity Report (SAR) Filing Deadlines 47

Retention of Suspicious Activity Report (SAR) Filings 48

The Travel Rule under the Bank Secrecy Act (BSA) 49
Suspicious Activity Report (SAR) Maintenance and Confidentiality....................50
Clearing Firm Relationship....................51
Training Programs....................52
Testing/Auditing Program....................54
Confidential Reporting by Employees of AML Non-Compliance....................55
Monitoring Employee Conduct and Accounts....................56
Senior Management Approval of AML Program 57

Overview

Anti-money laundering efforts are the responsibility of all associated individuals, from Senior Management to sales assistants. Spire is dedicated to a company-wide effort to detect and deter activities that could facilitate money laundering or the funding of terrorist or criminal activities.

Our CCO and our AML Principal will work together to see that our AML Program is monitored, reviewed, tested, and is appropriate for our business, and that we maintain appropriate documentation evidencing such efforts.

Our annual continuing education program will contain a specific AML requirement for both registered and non-registered individuals.

All registered and appropriate non-registered personnel will receive our policy on money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Senior Management appropriately complies with all laws and regulations designed to combat money laundering, including the reporting of (a) currency transactions, (b) utilization of certain monetary instruments and (c) other suspicious activities.

It is the responsibility of Senior Management, the Compliance Department, all supervising principals, and all registered representatives, and non-registered individuals (i.e., surveillance, etc.), to prevent this firm from being utilized by money launderers, as the consequences of non-compliance are severe, including significant criminal, civil, and disciplinary penalties.

Our anti-money laundering program is not a separate and distinct compliance area. All existing procedures and review policies incorporated into our AML program form the basis for an overall money laundering prevention program to ensure that this compliance effort reaches all appropriate areas of our business.

Compliance Officer Contact Information

FINRA Rule 3310 requires that each member firm provides to FINRA up-to-date contact information for the individual, or individuals, responsible for implementing the day-to-day operations and internal controls of the member's anti-money laundering program to ensure that information requests made on behalf of law enforcement agencies by FinCEN reach relevant financial institutions.

Our CCO will provide FINRA with the following information as it relates to the individual responsible for such activities, and that the information remains current. This information is entered into the FINRA Contact System (FCS) on the FINRA Gateway system and must include the following:

- Name of our AML Principal;   Jeff Ameen
- Title; AVP Compliance
- Mailing address; 7901 Jones Branch Dr., #800 McLean, VA 22102
- E-mail address; Jeff.Ameen@spireip.com
- Telephone number; and 703-657-6071

The information maintained on the FCS must be reviewed at least annually to ensure that it is current and correct.

Any change in the individual designated as our AML Principal should be made on the FCS within 30 days of such change. Should FINRA request any contact information, our AML Principal will ensure such information is provided within 15 days of such request.

Compliance Officer Designation and Duties

Responsibility

Senior Management, by annually signing and approving our AML Program, also approves the individual given AML Principal responsibilities.

Procedure

We have designated a specific individual (our AML Principal) as our Anti-Money Laundering Program Compliance Officer. This individual has been given full responsibility for the continual development and enforcement of our AML program.

The AML Principal has been named based on their experience, knowledge and ongoing continuing education efforts (through reading materials, web site resources and general review of all AML rules, training, regulations and requirements). The responsibilities given to our AML Principal include:

- monitoring for compliance of all AML areas by all employees
- structuring an appropriate AML training program for all registered employees
- determining which non-registered individuals are also required to avail themselves of our AML training program
- ensuring that AML directives are appropriately disseminated throughout the firm to all appropriate individuals
- internal Suspicious Activity Reports-SF (“SAR-SFs”) investigations
- filing of Suspicious Activity Reports-SF (“SAR-SFs”)
- ensuring that all Office of Foreign Assets Control (“OFAC”) checks are accomplished and documented
- ensuring that any other background checks undertaken are accomplished and documented
- ensuring that all documented and/or non-documented client identification is appropriately maintained in client files
- filing information-sharing notices when sharing AML-related information with other financial institutions
- responding (within required timeframes) to all governmental and regulatory agencies for information concerning any accounts we may hold
- maintaining records concerning the above and any other AML activities (minimally for a 5-year period after account closing)

Our AML Principal is responsible for maintenance of records relating to all of the above, as well as any other AML efforts.

Additionally, our AML Principal will oversee the testing of all our AML procedures, annually, to determine that all our AML procedures and requirements are appropriately undertaken and documented. Documentation of all testing findings, including any remedial steps taken where required, will be documented.

Emergency Telephone Notification to the Government

Responsibility

Our AML Principal has the responsibility for ensuring that, when necessary or deemed appropriate, emergency telephone notification regarding possible money laundering activity is made to the appropriate governmental agency.

Procedure

During the conduct of due diligence efforts prior to opening an account, or based on specific activities in an already-opened account, our AML Principal is responsible for making a determination whether federal law enforcement should be contacted by telephone. Such contact is mandatory should any of the following occur

- A legal or beneficial account holder or person with whom the account holder is engaged in a transaction is listed on, or located in, a country or region listed on the OFAC list
- An account is held by an entity that is owned or controlled by a person or entity on the OFAC list
- A customer attempts to use bribery, coercion or similar means to open an account or carry out a suspicious activity
- A customer appears to be trying to move illicit cash out of the government's reach
- There is reason to believe a customer is about to use the funds to further an act of terrorism

Our AML Principal will make all such calls, first contacting the OFAC Hotline at 1-800-540-6322.

Other contact numbers retained by our AML Principal and disseminated to all Senior Management include

- Local Hotline Number: (202) 622-2490
- Local U.S. Attorney's Office - Eastern District of VA - (804--819-5400)
- Local FBI Office - Washington DC (202-278-2000)
- Local SEC Office - Washington, DC (202-551-6000)

Suspicious Activity Reports-SF (SAR-SFs) may still be required even if information is provided over the Financial Institutions Hotline. The Hotline is intended to provide law enforcement and other authorized recipients of SAR-SF information the essence of the suspicious activity in an expedited manner. Forwarding information via the hotline is voluntary and does not affect our responsibility to file a SAR-SF in accordance with applicable regulations.

We will maintain appropriate documentation in the files concerning all such telephone notifications, indicating the findings that led to the call, documents reviewed (evidenced by initials and dates), the results of any such calls and all follow-up activities, as warranted.

Giving Information to Federal Law Enforcement Agencies and Other Financial Institutions

<u>Policy Requirements</u>

Requests under USA PATRIOT Act Section 319(b) are different from the requests made by the Financial Crimes Enforcement Network (FinCEN) under Section 314(a). Section 319 states that firms must respond to law enforcement requests to produce domestic and foreign bank records within seven calendar days.

<u>Procedures and Documentation</u>

Our AML Principal will ensure that FINRA's "FCS" System is always maintained in a current manner so that all FinCEN requests are received by the designated "point of contact" person.

As required under USA PATRIOT Act Section 314, we will respond to all FinCEN requests for information about accounts or transactions by reporting the identity of the specified individual or organization, the account number, all identifying information provided by the account holder when the account was established, and the date and type of transactions.

We will report to FinCEN (via FinCEN's Web-based 314(a) Secure Information Sharing System) as soon as possible, but no later than 14 days after receipt of a request, any account matches relating to Section 314 inquiries (and, if so requested, via email to patriot@fincen.treas.gov, by calling the Financial Institutions Hotline (1-866-556-3974) or by any other means that FinCEN specifies).

For any named suspects (FinCEN list "matches") our AML Principal will ensure that we query our records for data matches, including accounts maintained by the named subject during the preceding 12 months and transactions conducted within the last 6 months.

Our AML Principal will document and retain all FinCEN/Law Enforcement communications, ensuring that all responses are made within the appropriate timeframe. Regardless of whether there was anything required to be reported to FinCEN, our AML Principal will ensure that we maintain sufficient documentation regarding all searches by printing a search self-verification document from FinCEN's 314(a) Secure Information Sharing System confirming that we searched the 314(a) subject information against our records (utilizing FTNI within Spire Access) or maintaining a log indicating the date of the request, the number of accounts searched, the name of the individual who undertook the search and an indication whether or not a match or matches was/were found.

<u>Procedure</u>

1. Log into FinCEN system and download search request (.csv file) list.
2. Save search request in - W Drive > Spire Compliance > AML > FinCEN.
3. Run search request through upload in Spire Access
4. No hits - download and save to FinCEN file
5. Hits - report as required to FinCEN. - save in FinCEN folder

National Security Letters (NSLs)

Procedures and Documentation

National Security Letters (NSLs) are written investigative demands 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 from Spire.

Our AML Principal will ensure that AML training stresses that all NSL information remains 100% confidential, and limit the dissemination of any NSLs received on a strict “need to know” basis. Any individuals who have treated NSLs inappropriately will be terminated and a determination will be made as to whether such a breach of policy will require the filing of a Suspicious Activity Report (SAR).

In addition, our AML principal will ensure that any SARs filed after receipt of a National Security Letter contain NO reference to the receipt or existence of a NSL.

Grand Jury Subpoenas

<u>Procedures and Documentation</u>

Our AML Principal will ensure the proper handling of any subpoena we may receive as part of a grand jury's investigative proceeding.

While the receipt of a subpoena does not automatically require us to file a SAR, our AML Principal will undertake a risk assessment review of the customer(s) involved to determine if activities are suspicious, in which case we will file a SAR.

All subpoenas and any subsequent SAR filings will be dealt with by as few individuals as possible, each of whom will be fully aware of the fact that they cannot directly or indirectly disclose to the person(s) subject to the subpoena the existence of the subpoena, its contents, or the information used for our response. All individuals involved are advised that failure to adhere to this strict confidentiality requirement may result in termination, as well as federal criminal charges.

Our AML Principal will also ensure that any SAR filed in response to a subpoena may not contain any reference to the receipt or existence of a subpoena, but contains only detailed information about the facts and circumstances of our internal investigation and the suspicious activity uncovered.

Sharing Information with Other Financial Institutions

<u>Procedures and Documentation</u>

Our AML Principal ensures that all AML-related information shared with other financial institutions complies with the rules and regulations in the USA PATRIOT Act and FINRA Rule 3310.

Our AML Principal and other members of Senior Management will decide if we will share information about those suspected of terrorist financing and money laundering with other financial institutions to determine whether to establish or maintain an account or engage in a transaction on behalf of the account.

Our AML Principal must ensure that both we and the firm with which we intend to share the information (including, if applicable, our clearing firm and affiliated financial institutions) have filed an initial notice with FinCEN use the notice form found at https://bsaefiling.fincen.treas.gov/main.html. We will maintain documentation regarding our initial notice filings and copies of filings made by the entity with which we will share information in our AML files.

Because the initial notice expires within one year, we, along with the sharing entity, will file continuation notices if we continue to share information, retaining copies of all such continuation notice filings in our AML files.

Another way to determine that the entity with which we share information has filed the requisite notices (initially and annually thereafter) is to refer to FinCEN's published quarterly list of USA PATRIOT Act Section 314(b) participants available at https://www.fincen.gov/ns/314b/noti020414.pdf. We will maintain copies of all such verifications in our AML files, evidencing the review with initials and dates.

We will review our files annually to ensure that any SAR filings have been removed from client files and are maintained separately and securely. We will maintain documentation of all such reviews in the AML files, indicating what was reviewed, the dates of such reviews, the name of the individuals conducting the review and any findings and corrective measures taken, if any.

Our AML training materials and Annual Compliance Meeting will instruct attendees that NO information may be shared with any financial institution without first discussing the matter with our AML Principal.

We will also share information about particular suspicious transactions with our clearing broker (should we utilize the services of a clearing firm) to determine whether one or both firms should file a SAR. Our AML Principal will maintain documentation of these discussions.

Whenever we file a SAR for a transaction handled by both this firm and another financial institution, we may share a copy of the filed SAR with the other financial institution.

(The only time when it would be deemed inappropriate to share such a SAR filing is when the filing concerns the other financial institution or one or more of its employees).

Our AML training and other compliance efforts will make clear to all employees that all SAR filings are to be maintained on a confidential basis. NO SARs may be kept in client files. Our AML Principal is the ONLY individual permitted to maintain copies of all SAR filings. In addition, our AML Principal is the ONLY individual permitted to handle, review, and appropriately respond to any requests from any individual or entity requesting SAR information.

Our AML Principal will ensure that all records relating to sharing of information are retained for a five-year period.

Checking of OFAC and Other Government Lists

Responsibility

Our AML Principal will ensure that we have appropriate procedures in place to undertake all list checks required by the Office of Foreign Assets Control (OFAC) and those of other government entities.

Our AML Principal is also responsible for disseminating appropriate procedures if name checks are done in-house. If another entity (i.e., clearing firm, affiliated entity, third-party vendor) undertakes such checks on our behalf, the AML Principal will ensure that we are in compliance with the requirements under which we may rely on the performance by another financial institution for some, or all, of the elements of our Customer Identification Program (CIP). (See Anti-Money Laundering (AML) Program, Reliance on Another Financial Institution, section herein.)

Procedure

When processing a new account, we must ensure that a customer does not appear on a list provided by the government, such as the Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" List (SDN List), and ensure that the customer is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC Web Site.

The check conducted by our third-party vendor will indicate if a client appears on any of the referenced lists. If a client fails this check, documentation will be maintained in the client's AML folder on the "S" drive detailing the reason for the fail and information reviewed to determine a resolution. The date the check was conducted will be evidenced by the use of a notation on the account in our Spire Access system.

Regardless of whether we access these lists through various software programs to ensure speed and accuracy, use the services of an outside vendor, or manually check the lists, our AML Principal is responsible for maintaining adequate documentation as to how we undertake this compliance effort.

In the event that an OFAC check, or a check of any other list utilized, leads to a determination that a customer, or someone with or for whom the customer is transacting, is on the SDN List or is from, or engaging in transactions with, a person or entity located in an embargoed country or region, the transaction will be rejected, or we will block the customer's assets and file a Blocked Assets and/or Rejected Transaction form with OFAC. Our AML agreements with our custodians outline their obligation to scan all incoming and outgoing wires against any government lists. We will request an annual certification of such obligation.

All information relating to such findings will be documented in detailed fashion, with such documentation retained in our files). In such instances, the AML Principal will also ensure that we also notify OFAC by calling their Hotline at 1-800-540-6322.

Customer Identification Program (CIP)

Background

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 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).

Responsibility

Our AML Principal ensures that our AML program contains a Customer Identification Program (CIP) sufficient to meet the requirements of the USA PATRIOT Act, attendant FINRA rules and FinCEN's CDD Rule.

Our AML Principal also ensures that all appropriate associated personnel receive sufficient education and training on the requirements under our Customer Identification Program.

On an ongoing basis, designated supervising principals are responsible for ensuring that the individuals under their direct supervision are aware of the requirements and adhere to them.

Procedure

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
- An address
  - For an individual, a residential or business street address
  - - For other than an individual (corporation, partnership, trust, etc.), a principal place of business, local office or other physical location.

    - A P.O. Box may be used as the account mailing address. This is only permitted if the Legal address is also provided. In addition, any change to the P.O. Box or Legal address requires our client attestation procedures.
- 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

Without the proper documentation, Spire will refuse (i.e. NIGO) to open the account.

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 AML Principal and all appropriate supervisors will closely monitor accounts opened without a taxpayer identification number during the period of time the account is open prior to receipt of the number.

When it is not possible to examine original documents, every effort should be made to use a variety of identification verification methods.

Where documents 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.

However, registered and non-registered personnel alike are given training to be made aware of the requirement that in instances where a suspicion exists that a document shows, or seems to show, any obvious form of fraud, the reasonable belief that we know the customer's true identity cannot be deemed to exist.

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, or our AML principal upon review, may require some non-documented verification to back up the documented verification.

Documentary verification is required as follows:
<u>Individual</u>

- unexpired government-issued ID evidencing nationality or 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

<u>Non-Individual</u>

- 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 methods include, but are not necessarily limited to:

- 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 public database or other source. 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 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.

Definition of High Risk Accounts/Individuals: Accounts with an address outside of the US. Individuals (including beneficial owners) that are non-US citizens (either resident or non-resident). Our Spire Access system will capture the nationality of the non-US individual. Reports can then be run for periodic reviews by supervisors.

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. **Accounts identified as High Risk will also have a LexisNexis report run to determine if there is any negative news regarding the individual, Entity or Beneficial Owner.**

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 the event that a customer account fails a CIP check due to a failure to match the tax identification number in FTNI's RemitPro, a review will be performed to determine if an incorrect tax identification number was either provided or entered. The AML Principal will also request that the individual opening the account attest to the correct tax identification number via a signed Form W-9 for our records. The AML Principal will run a new CIP check using the corrected tax identification number in conjunction with the information provided on the new account form. The information provided on the new W-9 attested to by the account holder will also be used to correct the tax identification number originally entered in the custodian system.

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.

Documentation of all such training and educational efforts will be retained in the files indicating dates, copies of training materials utilized, method of delivery (i.e. annual compliance meeting, AML annual training, CE, compliance manuals, compliance alerts, on-line training, etc.) and names of all individuals who received the training.

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 via FTNI's RemitPRO/RiskAlert, will be retained in those data bases.

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 copy of, or 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. We will maintain records of all identification information for at least 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.

Customer Notification

Responsibility

Our AML Principal working with supervising principals will craft documentation in the account opening process that provides that all customer notification as required under FINRA Rule 3310 is appropriately delivered.

Additional information regarding the Customer Identification Program Notice can be obtained at: http://www.finra.org/industry/customer-identification-program-notice

Procedure

Notice will be provided on our client New Account Forms that Spire is requesting information from them as required by federal law.

Important Information You Need to Know about Opening a New Account

To help the government fight the funding of terrorism and money laundering activities, federal law requires financial institutions to obtain, verify, and record information that identifies each person who opens an account.

This Notice answers some questions about this broker/dealer's Customer Identification Program.

What types of information will you have to provide?

At the time you open an account with us, we are required to collect information such as the following from you:

- Your name
- Your date of birth
- Your address
- An identification number
    - U.S. Citizen: taxpayer identification number (social security number or employer identification card)

- Non-U.S. Citizen: taxpayer identification number, passport number, and country of issuance, alien identification number or government issued identification showing nationality, residence and a photograph of you.

You may also need to show your driver's license or other identifying documents.

A corporation, partnership, trust or other legal entity may need to provide other information such as its principal place of business, local office, employee identification number, certified articles of incorporation, government-issued business license, a partnership agreement or a trust agreement.

U.S. Department of the Treasury, Securities and Exchange Commission, FINRA and New York Stock Exchange rules already require you to provide most of this information. These rules also may require you to provide additional information, such as your net worth, annual income, occupation, employment information, investment experience and objectives, and risk tolerance.

What happens if I do not provide the information requested or my identity cannot be verified?

We may not be able to open an account or carry out transactions for you. If we have already opened an account for you, we may have to close it.

Closing Account after Failure to Verify Customer Identity

Responsibility

Our AML Principal ensures that accounts are appropriately handled in instances of our inability to verify a customer's identity.

Procedure

Spire will not open any account(s) until proper documentation is received.

Customers Who Refuse to Provide Information

Procedures and Documentation

Our AML Principal will be responsible for providing training to that all registered personnel appropriately handle account openings when faced with customers who refuse to provide the required information. In addition, everyone's immediate supervising principal is responsible for ongoing oversight of these situations and that they are handled according to the rules and regulations as well as with our internal policies and procedures.

Our policy is to NOT open an account for a potential or existing customer who refuses to provide the required information, or appears to have intentionally provided misleading information. All such instances must be reported to our AML Principal who may, within the 30-day opening period, decide to close any existing accounts with which the individual or entity is involved.

In addition, each individual's immediate supervising principal is responsible for ongoing oversight to ensure these situations are handled according to the firm's policies and procedures.

In addition, our AML Principal will determine whether to file a Suspicious Activity Report (SAR) with documented evidence with FinCEN.

Investigations will involve our AML Principal, the registered representative's direct supervising principal, and the registered representative. If necessary, additional Senior Management members may be included and a determination may be made to also bring in legal counsel.

Our AML Principal will maintain documentation of all such matters, noting how the final decision was reached and initialing and dating all documents reviewed.

Freezing of Accounts

Procedures and Documentation

Our AML Principal will make the final decision regarding the freezing of any account due to suspected money laundering or other suspicious activity.

To avoid prematurely alerting any individual potentially involved in illegal activities, we will not freeze any accounts we suspect may be engaged in money laundering or terrorist activities without first contacting FinCEN and seeking advice on how to proceed.

We will maintain careful notes concerning any such FinCEN conversation undertaken by our AML Principal (or other appropriate principal specifically designated to make such a call), and we will act appropriately as FinCEN directs us. If necessary, we will contact other regulators and law enforcement agencies concerning a decision to freeze an account where terrorist activities may be involved, and document such activities in our AML files.

Reliance on Another Financial Institution

Procedures and Documentation

When we rely on another financial institution for some or all of the elements of our Customer Identification Program (CIP), our AML Principal oversees such performance to ensure compliance with the USA PATRIOT Act and FINRA Rule 3310.

Regardless of whether we currently rely on another financial institution for assistance with our CIP Program, we have put these policies and procedures in place to readily be in compliance should the situation change.

When we rely on another financial institution (affiliated or non-affiliated) for any elements of our CIP Program, our AML Principal will ensure that the following records are maintained, with the review of each evidenced by initials and dates:

- A written description of which elements of our CIP Program another financial institution is administering on our behalf;
- The name of the financial institution;
- A written document indicating why Senior Management and our AML Principal feel that such reliance is reasonable, as the rules require that reliance on another institution must be reasonable under the circumstances;
- Documentation that the financial institution upon which we are relying is subject to a rule implementing the anti-money laundering compliance program requirements of the USA PATRIOT Act;
- Documentation that the financial institution upon which we are relying is regulated by a federal functional regulator (i.e., the SEC, the CFTC, the Board of Governors of the Federal Reserve System, the OCC, the Board of Directors of the Federal Deposit Insurance Corporation, the Office of Thrift Supervision or the National Credit Union Administration); and
- A copy of a contract between this firm and the financial institution upon which we are relying whereby that financial institution agrees to certify annually to us that it has implemented its anti-money laundering program and that it, or its agent, will perform specified requirements of our CIP Program.

When relying on another financial institution, we will not be held responsible for the failure of the other financial institution to adequately fulfill our CIP responsibilities, provided that we can establish that our reliance was reasonable and that we have obtained the requisite contracts and certifications.

Unless ALL of the conditions set forth in Section 326 of he USA PATRIOT Act (***which prescribes regulations establishing minimum standards for financial institutions and their customers regarding the identity of a customer that shall apply with the opening of an account at the financial institution***) are met, we remain solely responsible for applying our CIP Program to each customer in accordance with Section 326.

Customer Due Diligence

On May 11, 2016, FinCEN adopted a final rule on Customer Due Diligence Requirements for Financial Institutions (CDD Rule) to clarify and strengthen customer due diligence for covered financial institutions, including broker-dealers. The Rule becomes effective on May 11, 2018.

In its CDD Rule, FinCEN identifies four components of customer due diligence: (1) customer identification and verification; (2) beneficial ownership identification and verification; (3) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and (4) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information. As the first component is already an AML program requirement (under the CIP Rule), the CDD Rule focuses on the other three components.

Specifically, the CDD Rule focuses particularly on the second component by adding a new requirement that covered financial institutions establish and maintain written procedures as part of their AML programs that are reasonably designed to identify and verify the identities of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.

Under the CDD Rule, member firms must obtain from the natural person opening the account on behalf of the legal entity customer, the identity of the beneficial owners of the entity. In addition, that individual must certify, to the best of his or her knowledge, as to the accuracy of the information. FinCEN intends that the legal entity customer identify its ultimate beneficial owner(s) and not "nominees" or "straw men."

Once member firms obtain the required beneficial ownership information, the CDD Rule requires that firms verify the identity of the beneficial owner(s) – in other words, that they are who they say they are – and not their status as beneficial owners through risk-based procedures that include, ***at a minimum, the elements required for CIP procedures for verifying the identity of individual customers****. Such verification must be completed within a reasonable time after account opening. Member firms may rely on the beneficial ownership information supplied by the individual opening the account, provided that they have no knowledge of facts that would reasonably call into question the reliability of that information.*

The required records to be created and maintained must include*:*

(i) for identification, any identifying information obtained by the member firm pursuant to the beneficial ownership identification requirements of the CDD Rule, including without limitation the certification (if obtained); and

(ii) for verification, a description of any document relied on (noting the type, any identification number, place of issuance and, if any, date of issuance and expiration), of any non-documentary methods and the results of any measures undertaken, and the resolution of each substantive discrepancy. In addition to complying with existing SEC and FINRA record retention requirements, member firms must maintain the records collected for identification purposes for a minimum of five years after the account is closed, and for verification purposes, for five years after the record is made.

The CDD Rule also addresses the third and fourth components, which FinCEN states "are already implicitly required for covered financial institutions to comply with their suspicious activity reporting requirements," by amending the existing AML program rules for covered financial institutions to explicitly require these components to be included in AML programs as a new "fifth pillar." These requirements are discussed further below.

In addition to the information collected under the written Customer Identification Program, FINRA Rules 2090 (Know Your Customer) and 2111 (Suitability) and the 4510 Series (Books and Records Requirements), and Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3(a)(9) (Beneficial Ownership regarding Cash and Margin Accounts), 17a-3(a)(17) (Customer Accounts) and Regulation Best Interest, we have established, documented and maintained written policies and procedures reasonably designed to identify and verify beneficial owners of legal entity customers and comply with other aspects of the Customer Due Diligence (CDD) Rule. We will collect certain minimum CDD information from beneficial owners of legal entity customers.[1] We will understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile. We will conduct ongoing monitoring to identify and report suspicious transactions, and, on a risk basis, maintain and update customer information.

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

At the time of opening an account for a legal entity customer, the representative will identify any individual that is a beneficial owner of the legal entity customer by identifying any individuals who directly or indirectly own 25% or more of the equity interests of the legal entity customer, and any individual with significant responsibility to control, manage, or direct a legal entity customer. The following information will be collected for each beneficial owner:

(1) the name;

(2) date of birth (for an individual);

(3) an address, which will be a residential or business street address (for an individual), or an Army Post Office (APO) or Fleet Post Office (FPO) box number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address); and

(4) an identification number, which will be a Social Security number (for U.S. persons), or one or more of the following: a passport number and country of issuance, or other similar identification number, such as an alien identification card number, or number and country of issuance of any other government-

issued document evidencing nationality or residence <u>and</u> bearing a photograph or other similar safeguard (for non-U.S. persons).

For verification, we will describe any document relied on. We will also describe any non-documentary methods and the results of any measures undertaken.

b. Understanding the Nature and Purpose of Customer Relationships

FinCEN states that the CDD Rule requires that firms must necessarily have an understanding of the nature and purpose of the customer relationship in order to determine whether a transaction is potentially suspicious and, in turn, to fulfill their SAR obligations. To that end, the CDD Rule requires that firms understand the nature and purpose of the customer relationship in order to develop a customer risk profile. The customer risk profile refers to information gathered about a customer to form the baseline against which customer activity is assessed for suspicious transaction reporting. Information relevant to understanding the nature and purpose of the customer relationship may be self-evident and, depending on the facts and circumstances, may include such information as the type of customer, account or service offered, and the customer's income, net worth, domicile, or principal occupation or business, as well as, in the case of existing customers, the customer's history of activity. The CDD Rule also does not prescribe a particular form of the customer risk profile. Instead, the CDD Rule states that depending on the firm and the nature of its business, a customer risk profile may consist of individualized risk scoring, placement of customers into risk categories or another means of assessing customer risk that allows firms to understand the risk posed by the customer and to demonstrate that understanding.

We will conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, maintain and update customer information, including information regarding the beneficial ownership of legal entity customers, using the customer risk profile as a baseline against which customer activity is assessed for suspicious transaction reporting. Our suspicious activity monitoring procedures are detailed within Section 11 (Monitoring Accounts for Suspicious Activity).

Foreign Correspondent Accounts and Foreign Shell Banks

Spire's policy is that we will not establish, maintain, administer or manage correspondent accounts for foreign banks. We will monitor for this during our supervisory review of all new accounts being opened.

We will identify foreign bank accounts and any such account that is a correspondent account (any account that is established for a foreign bank to receive deposits from, or to make payments or other disbursements on behalf of, the foreign bank, or to handle other financial transactions related to such foreign bank) for foreign shell banks by a supervisory review prior to the opening of any account. Upon finding or suspecting such accounts, firm employees will notify the AML Compliance Person, who will terminate any verified correspondent account in the United States for a foreign shell bank. We will also terminate any correspondent account that we have determined is not maintained by a foreign shell bank but is being used to provide services to such a shell bank. We will exercise caution regarding liquidating positions in such accounts and take reasonable steps to ensure that no new positions are established in these accounts during the termination period.

Private Banking Accounts/Senior Foreign Political Figures

Policy Requirements

Spire's policy is not to open or maintain private banking accounts.

A "private banking" account is an account that requires a minimum deposit of $1,000,000, is established for one or more individuals, and is assigned to, administered or managed by, in whole or in part, an officer, employee, or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account.

A "senior foreign political figure" includes a current or former senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not); a senior official of a major foreign political party; or a senior executive of a foreign-government-owned commercial enterprise; a corporation, business or other entity formed by or for the benefit of any such individual; an immediate family member of such an individual; or any individual publicly known, or actually known by the firm, to be a close personal or professional associate of such an individual.

Procedures and Documentation

We do not open or maintain private banking accounts.

If we discover information indicating that a particular account holder may be a senior foreign political figure, and upon taking additional reasonable steps to confirm this information, we determine that the individual is, in fact, a senior foreign political figure, we will conduct additional enhanced due diligence to detect and report transactions that may involve money laundering or the proceeds of foreign corruption. This may lead to additional heightened surveillance of the account, restrictions on the account or terminaiton of the account.

Additional Areas of Risk

Responsibility

Our AML Principal and other members of Senior Management are responsible for reviewing all areas of our business to identify potential money laundering risks that may not be covered in the AML policies and procedures currently in place. We will conduct such a review at least annually, along with our annual independent audit, taking into consideration the nature of our business, our clients, the size and geographical location of our firm and any other indicators deemed appropriate to take into account.

Our AML Principal will be responsible for updating any policies or procedures based on the annual review.

Monitoring Accounts for Suspicious Activity

We will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business. (Red flags are identified in Section.) Monitoring will be conducted through the following methods:

We will conduct ongoing monitoring, on a weekly basis, utilizing reports available on the NFS Streetscape and Pershing DBS NetX360 Systems. These reports provide details on any money movements which their inherent rulesets would flag for further review if they appear to be suspicious. These weekly reports, whether results are returned or not, will be saved on Spire's shared drive.

Furthermore, both NFS and Pershing DBS will alert us to suspicious activity they detect on their respective systems. If and when suspicious activity is discovered via the reports described above, and/or through notification by NFS and/or Pershing DBS, we will commence an investigation of the reported transaction(s) in order to determine if a SAR is required to be filed.

The customer risk profile will serve as a baseline for assessing potentially suspicious activity. The designated AML Compliance Associate will be responsible for this monitoring, will review any activity that Spire's monitoring systems detect, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

Account holders deemed as "high-risk" individuals and/or entities, such as resident and non-resident aliens, Politically Exposed Persons ("PEPs"), and/or beneficial owners of entity accounts, especially where the entity is a cash-intensive business, will have heightened scrutiny surrounding their account activity.

We will also conduct the following reviews when the monitoring system detects suspicious activity, or when it is alerted by NFS and/or Pershing DBS to suspicious activity:

- Gather Customer Due Diligence ("CDD") information of the account holder(s) and all standing wire instructions for the account(s) in question.
- Compile account activity and wire transfer history for the account over an extended time-frame for a broader analysis of the activity.
- Ascertain whether there were any cybersecurity-related incidents for the account(s) in question.
- Contact the account custodian for information surrounding the account activity.
- If needed, contact the account holder and inquire about the wire activity (i.e. did the account holder have knowledge and/or authorize the wire; if so, what was the reason the wire was made).

We will document the monitoring and reviews as follows:

The weekly reports run on NFS Streetscape and Pershing DBS NetX360 will be saved to Spire Compliance's AML file on the shared drive. If further reviews are called for based upon the result(s) in the weekly report(s), the information gathered from the review as well as a write-up of the review will be saved in the same location on the shared drive. If it is determined that a SAR needs to be filed, Spire will file the SAR on the BSA's E-File System. A copy of the SAR and the filing confirmations will be saved on the shared drive.

The AML Compliance Person or his or her designee will conduct an appropriate investigation and review relevant information from internal or third-party sources before a SAR is filed. Relevant information can include, but not be limited to, the following:

- A review of the customer risk profile
- A review of the wire activity in the account(s) in question over an extended time frame.
- A review of standing wire instructions.
- OFAC search results performed on the account holder.
- Re-verification of account holder's identity.
- Determining beneficial owners, if an entity account, and re-running background and OFAC checks.
- If an entity account, determining the nature of the business.

Once the relevant information has been reviewed and an internal report has been drafted, a determination will be made on whether a SAR needs to be filed. In the event that a SAR needs to be filed Spire will file the SAR on the BSA's E-File System. A copy of the SAR and the filing confirmations will be saved on the shared drive.

Cybersecurity-related events have their own procedures for Spire staff to follow in an effort to contain and evaluate potential damages including, but not limited to, unauthorized transfers of funds and/or the unauthorized dissemination of Personally Identifiable Information ("PII").

When a cybersecurity event occurs, or is discovered at one of the branch offices, it is to be reported to Spire Operations, which will then open a ticket in Laserfiche Forms ("LFF"). The ticket will contain pertinent details of the event, including what occurred, how the event was discovered, and the processes taken to remedy the situation.

Once this ticket is submitted, it will go through review and approval by Spire Operations. Following approval of the procedures by Spire Operations, the ticket will then be forwarded for an additional layer of review by the AML Principal. During the course of this review, the AML Principal will review the procedures taken by Spire Operations and, given the nature of the cybersecurity event, whether a Suspicious Activity Report ("SAR") should be filed with FinCEN. If the AML Principal is of the belief that the cybersecurity event warrants the filing of a SAR, the AML Principal will file the SAR with FinCEN and also make a note of the filing and its filing number on the LFF cybersecurity ticket.

Red Flags

Responsibility

Our AML Principal will be responsible for providing all registered personnel with adequate training in spotting potential red flags that could trigger the need for a more in-depth review prior to opening an account or be an indication of money laundering or other illegal activities.

In addition, each individual's immediate supervising principal is responsible for ongoing oversight to ensure these situations are handled according to rules and regulations and our internal policies and procedures.

Potential Red Flags

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

- The customer exhibits unusual concern about the firm's compliance with government reporting requirements and the firm's AML policies, particularly with regard to his or her identity, type of business and assets, or the customer is reluctant or refuses to reveal any information concerning business activities or furnishes unusual or suspect identification or business documents
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy or are inconsistent with the customer's stated business or investment strategy
- The information provided by the customer that identifies a legitimate source for funds is false, misleading or substantially incorrect
- Upon request, the customer refuses to identify or fails to indicate any legitimate source of his or her funds and other assets
- The customer, or a person publicly associated with the customer, has a questionable background or is the subject of news reports indicating possible criminal, civil or regulatory violations
- The customer exhibits a lack of concern regarding risks, commissions or other transaction costs
- The customer appears to be acting as an agent for an undisclosed principal but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of their industry
- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents or asks for exemptions from the firm's policies relating to the deposit of cash and cash equivalents
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers
- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the Financial Action Task Force (FATF)

- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity
- The customer's account shows numerous currency or cashier check transactions aggregating to significant sums
- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose
- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven
- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third-party or to another firm without any apparent business purpose
- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose
- The customer requests that a transaction be processed to avoid the firm's normal documentation requirements
- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, Regulation S stocks, and bearer bonds that, although legitimate, have been used in connection with fraudulent schemes and money laundering activity - such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity
- The customer's account shows an unexplained high level of account activity with very low levels of securities transactions
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose
- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer

Our AML training, will address the red flags noted above. All registered personnel and any unregistered individuals engaged in AML surveillance activities will receive such training to ensure their familiarity with possible money laundering activities so they can detect suspicious customer activities.

Further, such training instructs registered representatives in their responsibility to immediately alert either their direct supervising principal or our AML Principal upon detection of a possible red flag.

They are trained to understand that the final determination of whether the action is reportable or determined to be suspicious upon further investigation is not theirs to make. They are to alert appropriate individuals that an activity has occurred that requires assistance with further investigation.

We will maintain documentation of all such training, including copies of the training material, copies of handouts, if applicable, and dates and lists of individuals who received such training, as part of our AML books and records.

We will also maintain documentation of any red flag investigation, with results and further actions taken, if appropriate, including rationale for any further steps taken, such as requiring the gathering of additional information internally or from third-party sources, contacting the government, freezing the account or filing a SAR-SF, along with the final decision, as part of our AML books and records.

Filing a Suspicious Activity Report (SAR)

FINRA will assess firms' compliance with FinCEN's Customer Due Diligence (CDD) rule, which requires that firms identify beneficial owners of legal entity customers, understand the nature and purpose of customer accounts, conduct ongoing monitoring of customer accounts to identify and report suspicious transactions and, on a risk basis, update customer information.

With respect to the requirement to obtain beneficial ownership information, financial institutions will have to identify and verify the identity of any individual who owns 25 percent or more of a legal entity, and an individual who controls the legal entity.

On October 11, 2019, the SEC, the US Commodity Futures Trading Commission (CFTC), and the US Treasury Department's Financial Crimes Enforcement Network (FinCEN) issued a joint statement confirming that anti-money laundering and certain other obligations under the Bank Secrecy Act apply to firms' business activities involving **digital assets.**

The joint statement addressed the application of AML laws and rules to digital assets, regardless of whether those same digital assets also meet the definition of a "security" in the Securities Act of 1933 or a "commodity" in the Commodity Exchange Act. More specifically, the joint statement confirms that AML laws and rules apply to all activities involving digital assets, even if those assets are not subject to regulation by the SEC or CFTC—the digital asset "exchange" would have to file certain SARs with FinCEN when it reasonably suspects suspicious activity and also comply with certain other AML obligations.

Procedures and Documentation

Our AML Principal oversees all investigations to determine whether a SAR is required, as well as any actual SAR filings.

SAR filings are required under the Bank Secrecy Act (BSA) for any account activity conducted or attempted through our firm involving $5,000 or more where we know, suspect, or have reason to suspect that:

- The transaction involves funds derived from illegal activity or is intended or conducted to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation;
- The transaction is designed to evade any requirements of the BSA regulations;
- The transaction has no business or apparent lawful purpose, or is not the sort in which the customer would normally be expected to engage, and after examining the background, possible purpose of the transaction, and other facts, we know of no reasonable explanation for the transaction; or
- The transaction involves the use of the firm to facilitate criminal activity.

In high-risk situations, we will notify the appropriate government agency immediately and file a SAR with FinCEN. Securities law violations that are reported to the SEC or to a Self-Regulatory Organization

(SRO) may also be reported promptly to the local U.S. Attorney, as deemed appropriate by our AML Principal, other members of Senior Management, and/or legal counsel.

We will maintain files concerning any SAR investigation undertaken, indicating the activity that prompted the investigation, the names of individual(s) involved in such investigations, dates, review materials, etc. In addition, our documentation will include the rationale utilized to determine whether to file a SAR, as well as a copy of the filing.

We will not file SARs to report violations of federal securities laws or SRO rules by our employees or registered representatives that do not involve money laundering or terrorism, but will report them to the SEC or SRO.

Quarterly, our AML Principal will report all SAR filings to Senior Management and other appropriate control individuals, reminding such individuals of the strict confidentiality requirements of all SAR filings.

All SAR filings will also be reviewed to ensure that they have been filed within the appropriate timeframe.

SAR instructions are available on FinCEN's website at https://www.fincen.gov/sites/default/files/shared/fin101_instructions_only.pdf.

Notifications of SAR Filings

Procedures and Documentation

Our AML Principal will ensure that we adhere to all requirements surrounding SAR filing confidentiality and notification.

Anyone who is subpoenaed or required to disclose a SAR or the information contained in the SAR, except where disclosure is requested by FinCEN, the SEC, or another appropriate law enforcement or regulatory agency or an SRO overseen by the SEC*, is to DECLINE to produce the SAR or to provide any information that would disclose that a SAR was prepared or filed.

Our AML Principal will immediately notify FinCEN of any such request and our response, and maintain documentation concerning any such requests and communication with FinCEN, as part of our AML books and records.

* FINRA Regulatory Notice 12-08 states: "In a January 26, 2012, letter to FINRA, the SEC requested that all FINRA member firms make SARs and supporting documentation as well as any information that would reveal the existence of a SAR or any decision to not file a SAR available to FINRA."

Suspicious Transactions and Bank Secrecy Act (BSA) Reporting

Procedures and Documentation

Our AML Principal is responsible for filing Suspicious Activity Reports (SARs) as required under the Bank Secrecy Act.

Firms are required to file suspicious activities on Form SAR, available through the Treasury's web site at http://www.occ.treas.gov/sar.htm.

Our AML Principal is responsible for monitoring this website and other appropriate websites at least annually to ensure that we remain in compliance if any changes are made to the form or the filing requirements.

All registered personnel are advised (i.e., through our Annual Compliance Meeting, our anti-money laundering training program, or through any compliance alerts we disseminate) that SARs are confidential, and MAY NOT BE DISCLOSED to any person involved in the transaction.

The AML Principal ensures that we have in place a system for reporting transactions that we know or suspect are:

- Related to illegal activities;
- Designed to evade Bank Secrecy Act regulations; and
- Not apparently serving any business or lawful purpose.

In addition, our AML Principal will determine the transactions or account activities that warrant further investigation and make the final determination regarding the filing of a SAR. Where appropriate, the AML Principal may call on legal counsel to assist in making the final determination whether to file a SAR. Our AML Principal will maintain detailed documentation regarding any investigations taken to determine whether a SAR filing is required, including the final rationale made either for, or against, filing a SAR.

SAR Maintenance and Confidentiality

Policy Requirements

Our AML Principal ensures that all associated personnel are aware of the requirement to maintain confidentiality regarding all SAR filings.

Procedures and Documentation

All employees are advised (i.e., through our Annual Compliance Meeting, AML training, their supervising principals, etc.) of the serious consequences if a SAR and all accompanying supporting documentation is not maintained in a strictly confidential manner. They are advised that we are not to inform ANYONE outside of a law enforcement or regulatory agency or securities regulator about a SAR. The only exception is that SAR information may be shared with a parent entity or entities, both domestic and foreign (as noted in FinCEN's January 20, 2006, "Guidance on Sharing of Suspicious Activity Reports by Securities Broker-Dealers, Futures Commission Merchants, and Introducing Brokers in Commodities").

Prior to sharing SAR related information with an individual purporting to be affiliated with a legitimate law enforcement agency, we must receive written documentation that confirms that fact, and we must also verify the individual's credentials by contacting the agency by telephone.

Employees are also instructed that they and this firm are to deny any subpoena or other requests for SAR or SAR information except when such request comes from FinCEN, the SEC or another appropriate law enforcement or regulatory agency or an SRO overseen by the SEC. Our AML Principal will maintain documentation of all AML training covering this topic, indicating dates of such training, copies of training materials utilized, and names and CRD #s of individuals receiving such training.

Employees are advised to alert their immediate supervising principal, the AML Principal or other appropriate member of Senior Management immediately upon receipt of any such requests, as these are the only individuals authorized to determine the handling of such requests. We will retain documentation relating to all such requests, including initials, dates and written rationale of how the decision to respond was reached. Our AML Principal will immediately advise FinCEN of any such subpoena we receive, documenting all conversations for our files and maintaining records of all such communications.

If we utilize the services of a clearing firm, we will share information with it about suspicious transactions to determine whether a SAR should be filed. The only instance where such sharing would be deemed not appropriate would be when the SAR filing concerns the clearing firm or one or more of its employees. Our AML files will contain copies of all communication with our clearing firm regarding the filing of any SAR.

Our AML Principal will also ensure that all SAR filings and copies of all supporting documentation are segregated from other books and records we are required to maintain, thereby ensuring that there is no inadvertent disclosure of SAR filings.

SAR Filing Deadlines

Procedures and Documentation

Our AML Principal ensures that all SAR filing deadlines are met.

A SAR must be filed no later than 30 calendar days after the date of initial detection of the facts that constitute the basis for such filing.

To ensure that SAR filings are made in a timely manner, our AML Principal will review all current SAR investigations monthly to determine whether a date has been reached when the facts were deemed to constitute the basis for a filing.

If no suspect is identified on the date of initial detection, we may delay filing the SAR for an additional 30 calendar days pending identification of a suspect, but in no case will the reporting be delayed more than 60 calendar days after the date of initial detection. We will maintain documentation of the rationale for delaying the filing for an additional 30-day period in the files.

In order to be able to file a SAR electronically, our AML Principal must ensure that we have registered with FinCEN by logging onto http://bsaefiling.fincen.treas.gov.

Retention of Suspicious Activity Report (SAR) Filings

Our AML Principal ensures that we maintain copies of all SAR filings and the supporting documentation, as required under the Bank Secrecy Act (BSA).

Our AML Principal will retain copies of all SARs filed and the original or business-record equivalent of any supporting documentation for five years from the date of filing the SAR.

Our AML Principal will also identify and maintain supporting documentation and make such information available to FinCEN, as well as to any other appropriate law enforcement agencies or federal or state securities regulator, upon request.

Handling of Accounts for Which a SAR Has Been Filed

Procedures and Documentation

Our AML Principal will ensure that we appropriately handle all accounts for which a SAR has been filed as required under the Bank Secrecy Act.

Senior Management, with input from the Compliance Department, our AML Principal, and, if appropriate, with registered personnel handling the account, will determine how to handle transactions or account activity in an account that has had a SAR filed. All such accounts must be:

- Permanently closed;
- Temporarily frozen;
- Limited in activity; or
- Monitored daily pending final determination.

Quarterly, we will review all SAR filings to ensure that appropriate action has been taken on each account.

As part of our AML books and records, we will maintain documentation regarding who was involved in the review, dates of such review, and rationale for the final decision made on each account. We will also maintain records regarding advising appropriate individuals of the status of the accounts.

Suspicious Transactions and Bank Secrecy Act (BSA) Reporting

Procedures and Documentation

Our AML Principal is responsible for filing Suspicious Activity Reports (SARs) as required under the Bank Secrecy Act.

Broker-dealers are required to file suspicious activities on Form SAR, available through the Treasury's web site at http://www.occ.treas.gov/sar.htm.

Our AML Principal is responsible for monitoring this website and other appropriate websites at least annually to ensure that we remain in compliance if any changes are made to the form or the filing requirements.

All registered personnel are advised (i.e., through our Annual Compliance Meeting, our anti-money laundering training program, and through any compliance alerts we disseminate) that SARs are confidential, and MAY NOT BE DISCLOSED to any person involved in the transaction.

The AML Principal ensures that we have in place a system for reporting transactions that we know or suspect are:

- Related to illegal activities;
- Designed to evade Bank Secrecy Act regulations; and
- Not apparently serving any business or lawful purpose.

In addition, our AML Principal will determine the transactions or account activities that warrant further investigation and make the final determination regarding the filing of a SAR. Where appropriate, the AML Principal may call on legal counsel to assist in making the final determination whether to file a SAR. Our AML Principal will maintain detailed documentation regarding any investigations taken to determine whether a SAR filing is required, including the final rationale made either for, or against, filing a SAR.

Bank Secrecy Regulations - Special Measures

Responsibility

Our AML Principal will review Bank Secrecy Regulations to ensure that we are aware of all special measure requirements when dealing with foreign banks.

Procedure

It is Spire's intent to not open any correspondent bank accounts.

If we should find that any correspondent bank accounts had been opened, we will undertake the following:

Our AML Principal will provide a "One-Time Notification" when applicable informing them of the prohibition of doing business with certain Specified Banks under Section 311 of the Patriot Act.

Our AML Principal will ensure that, if a review of our correspondent accounts determines that we have established, maintained, administered or managed accounts for, or on behalf of, any of the above, such accounts will be immediately terminated. We will maintain documentation of such review and ensuing account termination in our files.

If, for any reason, we have or obtain knowledge that another correspondent account established, maintained, administered or managed by that financial institution in the U.S. for a foreign bank is being used by the foreign bank to provide banking services indirectly to any of the above, our AML Principal will work with appropriate members of Senior Management to ensure that the correspondent account is no longer used to provide such services, including when necessary, terminating the correspondent account.

Should any correspondent accounts require termination, we will take the following steps:

- The account will be terminated within a reasonable time
- No new positions will be permitted to be established within the account
- No transactions will be allowed to be executed within the account, other than those necessary to close the account, from the time the decision is made to terminate the account to final termination

Should a business decision be made at some later date to reestablish such a terminated account, our CCO and Senior Management will make a determination based on assurances that the account will not, in any manner, be utilized to provide banking services of any kind to any prohibited financial institutions (foreign banks). Our AML Principal will maintain documentation of these discussions and the rationale used to make the final determination.

Nothing in the BSA regulations requires us to maintain any records, to obtain any certification or to report any information not otherwise indicated herein or required by other regulatory laws or regulations.

High Risk and Non-Cooperative Jurisdictions

Responsibility

Our AML Principal will provide all appropriate registered personnel sufficient training concerning the issues raised by accounts located in problematic countries and that adequate procedures are in place for checking accounts against appropriate government lists.

Procedure

All accounts located in problematic countries will be carefully scrutinized, and we will maintain documentation in the file evidencing such scrutiny. **We will look to our clearing firms for guidance on where they will permit accounts to be located.**

We may also check, or have a third-party check on our behalf, the lists and accompanying narrative information of the Financial Action Task Force (FATF) available at http://www.fatf-gafi.org/countries/, and FinCEN available at http://www.fincen.gov, as well as other available resources to determine problematic countries. We will factor this information into our decisions whether to open or maintain accounts based in these jurisdictions.

Currency Transaction Reports (CTRs)

Policy Requirements

Currency Transaction Reports (CTRs) are filed only for certain transactions involving currency, defined as *"coin and paper money of the United States or of any other country .. customarily used and accepted as a medium of exchange in the country of issuance."* Currency includes U.S. silver certificates, U.S. notes, Federal Reserve notes and official foreign bank notes that are customarily used and accepted as a medium of exchange in a foreign country.

Procedures and Documentation

Our AML Principal are responsible for seeing that CTRs are filed, when required, due to a violation of our prohibition against accepting currency.

Spire prohibits the receipt of currency and has the following procedures to prevent its receipt:

- We utilize our Annual Compliance Meetings, registered representative training materials, compliance alerts, supervisory oversight, etc., to impress upon all employees our firm's strict prohibition against accepting currency from any client or potential client. All affiliated personnel are advised that disciplinary sanctions, including the possibility of immediate termination, will occur upon the discovery of noncompliance with this prohibition.
- In any instance of cash deposits, our AML Principal will immediately undertake an investigation to determine the nature of such cash. We will maintain notes in the file concerning all such bank deposit review activities, including initialing and dating of all documents reviewed, dated notes of any discussions, etc.;
- If we determine that, despite our prohibition, currency has been received, our AML Principal will ensure that CTRs are filed with FinCEN for transactions involving currency that exceeds $10,000. We will treat multiple transactions as a single transaction if they total more than $10,000 during any one business day. We will retain copies of all CTR filings and information regarding the circumstances requiring such filing, in the files;
- In order to file the appropriate electronic CTR, our AML Principal will ensure we are registered with FinCEN (by logging on to http://bsaefiling.fincen.treas.gov); and
- In instances where currency was received despite our prohibition, the circumstances will be investigated and the individual involved will face sanctions, including the very likely possibility of termination.

Currency and Monetary Instrument Transportation Reports (CMIRs)

Policy Requirements

Currency and Monetary Instrument Transportation Reports (CMIRs) are filed for certain transactions involving monetary instruments that include the following: currency; travelers checks in any form; all negotiable instruments, including personal and business checks, official bank checks, cashier's checks, third-party checks, promissory notes and money orders, that are either in bearer form, endorsed without restriction, made out to a fictitious payee or otherwise in such form that title passes upon delivery; incomplete negotiable instruments that are signed but with the payee's name omitted; and securities or stock in bearer form or otherwise in such form that title passes upon delivery.

Procedures and Documentation

Our firm prohibits both the receipt of currency or other monetary instruments that have been transported, mailed or shipped to us from outside of the United States, and the physical transportation, mailing or shipment of currency or other monetary instruments by any means other than through the postal service or by common carrier. We will file a CMIR with the Commissioner of Customs if we discover that we have received or caused or attempted to receive from outside of the U.S. currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time (on one calendar day or, if for the purposes of evading reporting requirements, on one or more days). We will also file a CMIR if we discover that we have physically transported, mailed or shipped or caused or attempted to physically transport, mail or ship by any means other than through the postal service or by common carrier currency or other monetary instruments of more than $10,000 at one time (on one calendar day or, if for the purpose of evading the reporting requirements, on one or more days). We will use the CMIR Form provided on FinCEN’s website.

Recordkeeping

<u>Responsibility</u>

Our AML Principal will assist in developing tools and procedures, along with other departments, in order to monitor accounts to detect suspicious activity.

<u>Procedure</u>

Our AML Principal is responsible for ensuring that, as required under the Exchange Act Rule 17a-8 and Treasury's Bank Secrecy Act, all books and records relating to Spire Investment Partners' AML program are maintained for a minimum of five years from the date the account was closed.

Our AML Principal will oversee all recordkeeping issues.

Our AML Principal will undertake an annual review to ensure that required documentation is appropriately maintained, evidencing such review by documenting the findings and any corrective measures taken.

Records Required

Records maintained for a five-year period include, but are not necessarily limited to

- Details of any pre-SAR-SF filing investigations, including the final determination and how it was reached
- Documentation of due diligence efforts regarding client identity
- Documentation of information-sharing with other financial institutions
- Evidence of roles played by other financial institutions in our AML program
- Information regarding all red flag investigations
- Copies of AML materials utilized to ensure adequate AML training for all appropriate employees
- Documentation of amendments made to our AML program and any related policies and procedure changes
- Notes relating to reports to Senior Management relative to our AML efforts
- Copies of exception reports utilized to detect suspicious activities
- Travel rule documentation
- Copies of all SAR-SF, CTR, CMIR and FBAR filings (SAR filings are kept separately in a confidential location)
- Notes relating to any emergency calls made to federal law enforcement officials
- Any other appropriate materials required to document the enforcement of our AML program and related policies and procedures
- FinCEN Search requests and findings

Suspicious Activity Report (SAR) Filing Deadlines

Procedures and Documentation

Our AML Principal ensures that all SAR filing deadlines are met.

A SAR must be filed no later than 30 calendar days after the date of initial detection of the facts that constitute the basis for such filing.

To ensure that SAR filings are made in a timely manner, our AML Principal will review all current SAR investigations monthly to determine whether a date has been reached when the facts were deemed to constitute the basis for a filing.

If no suspect is identified on the date of initial detection, we may delay filing the SAR for an additional 30 calendar days pending identification of a suspect, but in no case will the reporting be delayed more than 60 calendar days after the date of initial detection. We will maintain documentation of the rationale for delaying the filing for an additional 30-day period in the files.

In order to be able to file a SAR electronically, our AML Principal must ensure that we have registered with FinCEN by logging onto http://bsaefiling.fincen.treas.gov.

Retention of Suspicious Activity Report (SAR) Filings

Our AML Principal ensures that we maintain copies of all SAR filings and the supporting documentation, as required under the Bank Secrecy Act (BSA).

Our AML Principal will retain copies of all SARs filed and the original or business-record equivalent of any supporting documentation for five years from the date of filing the SAR.

Our AML Principal will also identify and maintain supporting documentation and make such information available to FinCEN, as well as to any other appropriate law enforcement agencies or federal or state securities regulator, upon request.

The Travel Rule under the Bank Secrecy Act (BSA)

<u>Background</u>

Transfers of $3,000 or More under the Joint and Travel Rule

The Department of the Treasury's amendments to the Bank Secrecy Act facilitating tracing funds through the funds-transmittal process (travel rule) became effective on May 28, 1996.

<u>Responsibility</u>

Our AML Principal will ensure our compliance with all requirements under the BSA's travel rule.

<u>Procedure</u>

For transmittals of funds, including wire or electronic transfers, of three thousand dollars ($3,000) or more, sent or received by us, we must obtain and keep certain specified information concerning the transmitter and the recipient of those funds. Additionally, we must include this information on the actual transmittal orders.

Funds are never wired from Spire to client's accounts or elsewhere for the benefit of the client. All transmittals of funds are done via our clearing firms.

Whenever a client requests that money be wired from their account, we, as the financial institution acting on behalf of the transmitter (i.e. client), must include and send to our custodian - via electronic means, the following information in the wire transmittal order:

- the name of the transmitter - Which appears on the account.
- the account number of the transmitter (if account numbers are utilized)
- the address of the transmitter
- the identity of the transmitter’s financial institution
- the amount of the transmittal order
- the execution date of the transmittal order
- the identity of the recipient's financial institution;

Requests of transfers to third parties are treated differently (requiring additional documentation and verbal confirmation) than those that are being transferred to same registration (first party).

All wire transfers are executed via our clearing firm. Standardized templates on their cashiering platform require certain pieces of information - including those listed above.

Suspicious Activity Report (SAR) Maintenance and Confidentiality

Policy Requirements

Our AML Principal ensures that all associated personnel are aware of the requirement to maintain confidentiality regarding all SAR filings.

Procedures and Documentation

All employees are advised (i.e., through our Annual Compliance Meeting, AML training, their supervising principals, etc.) of the serious consequences if a SAR and all accompanying supporting documentation is not maintained in a strictly confidential manner. They are advised that we are not to inform ANYONE outside of a law enforcement or regulatory agency or securities regulator about a SAR. The only exception is that SAR information may be shared with a parent entity or entities, both domestic and foreign (as noted in FinCEN's January 20, 2006, "Guidance on Sharing of Suspicious Activity Reports by Securities Broker-Dealers, Futures Commission Merchants, and Introducing Brokers in Commodities").

Prior to sharing SAR related information with an individual purporting to be affiliated with a legitimate law enforcement agency, we must receive written documentation that confirms that fact, and we must also verify the individual's credentials by contacting the agency by telephone.

Employees are also instructed that they and this firm are to deny any subpoena or other requests for SAR or SAR information except when such request comes from FinCEN, the SEC or another appropriate law enforcement or regulatory agency or an SRO overseen by the SEC. Our AML Principal will maintain documentation of all AML training covering this topic, indicating dates of such training, copies of training materials utilized, and names and CRD #s of individuals receiving such training.

Employees are advised to alert their immediate supervising principal, the AML Principal or other appropriate member of Senior Management immediately upon receipt of any such requests, as these are the only individuals authorized to determine the handling of such requests. We will retain documentation relating to all such requests, including initials, dates and written rationale of how the decision to respond was reached. Our AML Principal will immediately advise FinCEN of any such subpoena we receive, documenting all conversations for our files and maintaining records of all such communications.

We will share information with our clearing firm about suspicious transactions to determine whether a SAR should be filed. The only instance where such sharing would be deemed not appropriate would be when the SAR filing concerns the clearing firm or one or more of its employees. Our AML files will contain copies of all communication with our clearing firm regarding the filing of any SAR.

Our AML Principal will also ensure that all SAR filings and copies of all supporting documentation are segregated from other books and records we are required to maintain, thereby ensuring that there is no inadvertent disclosure of SAR filings.

Clearing Firm Relationship

Responsibility

Our AML Principle will oversee any AML requirements undertaken on our behalf by our clearing firm.

Procedure

We will update and maintain documentation on any information exchanged (records, data and exception reports as necessary to comply with AML laws, etc.). The designated principal will document this review with initials and dates, and retain all documents relating to this firm and our clearing firm.

In the case of any agreement under which our clearing firm monitors customer activity on our behalf, our AML files will indicate (with dates and method of transmittal noted) that we have provided our clearing firm with proper customer identification information as required to successfully monitor customer transactions. Our AML Principal will ensure that these responsibilities are clearly set forth in our clearing agreement as required under FINRA Rule 3310. NFS and Pershing do run their own customer check on all account openings - independent of Spire's checks.

As a part of our clearing relationship, Spire has a contractual AML agreement in file (Laserfiche) for both NFS and Pershing regarding their obligations as well as ours as the correspondent firm. We will request annually, from each custodian, a confirmation of the obligations called for in our Correspondent Clearing Agreements.

We understand that the agreement will not relieve either this broker-dealer or our clearing firm from our independent obligation to comply with AML regulations.

FinCEN Inquiries Received by Our Clearing Firm

If our AML Principal is notified by our clearing firm of a potential match to a 314(a) target account transaction, the AML Principal will create a file to document the requests and any communications relevant to the request. Positive responses are coordinated with our clearing firm and communicated to the Financial Crime Enforcement Network (FinCEN). We will maintain documentation relating to any such FinCEN communications in the files.

Training Programs

Responsibility

Our AML Principal, in cooperation with our compliance department, will be responsible for the development of training that all affiliated personnel, registered as well as those non-registered individuals will be required to complete. Such training will provide sufficient AML training to understand the issues involved, and to be aware of our policies and procedures for complying with the USA PATRIOT Act and FINRA Rule 3310.

Procedure

Our AML Principal will develop the employee training program, with formal training taking place at least annually. The content of such training, delivery mechanisms, etc., will be based on our firm's size, customer base and resources.

Spire's AML training program has traditionally been included with our annual Firm Element program utilizing a 3rd party resource (QuestCE).

Based on feedback, potential areas of concern uncovered during routine reviews and the level of experience of the registered personnel, circumstances may require that certain individuals undergo additional specific periodic training relative to our money laundering prevention efforts.

Our AML Principal will maintain a list of all employees required to complete our AML training program and another list of any individuals required to undergo additional training for any reason (e.g., new to the industry, perceived problems with adhering to AML policies and procedures, specific surveillance training needs, etc.) and ensure that each individual completes the program within the appropriate time frame.

Our training will include how to detect unusual or suspicious transactions and how to maintain compliance with the various federal rules, regulations and reporting requirements. Our training will also include clear instructions about our internal policies and procedures and the steps that are required if an individual notes possible suspicious behavior or activity.

Registered personnel, and certain non-registered personnel, will be made aware through our training program of their role in our overall anti-money laundering efforts. The training may include some or all the following topics.

- Know your customer
- Potential indicators of suspicious activity
- Rules and regulations for reporting currency transactions
- Transportation of monetary instruments
- Suspicious activities
- Civil and criminal penalties associated with money laundering
- Recent developments in regulations
- New techniques in money laundering activity efforts
- New money laundering trends identified by various government agencies (i.e., FinCEN and FATF)

- How to identify red flags
- Signs of money laundering that may arise during the course of their duties
- What to do once a risk is identified
- Their role in our AML compliance efforts
- How to perform the role adequately and appropriately
- How to comply with our record retention policy
- The disciplinary consequences (including civil and criminal penalties) they may face for non-compliance with the USA PATRIOT Act

In addition, our training will include heightened risk verification issues. This training will stress the fact that, in certain instances, simple documentary or non-documentary client identification verification is not sufficient.

Supervisory personnel will also be given specific training to know that if a registered representative does not initially obtain sufficient information on a customer designated as a heightened risk, the account opening process is halted and the matter is discussed with the particular individual who opened the account. Continued failure to understand the requirements may result in additional training requirements for the individual involved and, in appropriate instances, for the supervisor, as well.

While our training may be intensified to include internal dissemination of educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos, our training program currently consists of the following.

Annually, all appropriately designated registered and non-registered personnel are required to complete the training program requirements that have been assigned to them

Our AML Principal will determine whether such training can be offered in-house with appropriate delivery mechanisms or whether an outside vendor's online training materials are more suitable for some, or all, instances.

If we use an outside vendor for some, or all, of our AML training requirements, our AML Principal will ensure that the vendor maintains sufficient records for us to be able to track the completion and testing results of all individuals required to take the training.

In general, our AML training files will contain the names of all individuals required to receive training, the levels and time frames of training required for each, evidence of notification to each individual regarding his or her requirements, the documentation of successful completion of required training, copies of communication with those who have not complied within the required time frame, method of training delivery, copies of training materials, etc.

Testing/Auditing Program

Responsibility

Our AML Principal will be responsible for arranging the appropriate testing and auditing of our AML program on an annual basis (calendar basis).

Procedure

Our AML Principal will determine whether we have sufficient independent internal individuals to undertake the testing and auditing of our AML program or whether we must retain an outside independent third-party for this requirement.   Currently we do utilize a third-party provider, Oyster Consulting, LLC for our annual AML review.

The AML Principal must also maintain appropriate documentation evidencing such testing and auditing in the file.

As required, our AML Principal will ensure that each of the recommendations made as a result of the testing/auditing are considered, and that appropriate adjustments to our AML program are made.

Confidential Reporting by Employees of AML Non-Compliance

Procedures and Documentation

Our AML training, will inform all employees that they are to immediately report any possible violations of the firm's AML compliance program to the AML Principal.

If any perceived or actual violation could implicate the AML Principal, employees are advised that the report should be made to their immediate or other appropriate supervising principal.

All AML training efforts will make clear to employees that any reports will remain confidential and that the reporting individual will suffer no retaliation or consequences for making the report.

Monitoring Employee Conduct and Accounts

Responsibility

Our CCO will monitor employee conduct and employee accounts in order to detect any possible engagment in any money laundering activities. The CCO will work in concert with our AML Principal (if the CCO is not also the AML Principal) as well as the representative's supervising principal.

Procedure

Our CCO will subject employee accounts to the same AML procedures as customer accounts.

Senior Management Approval of AML Program

<u>Procedures and Documentation</u>

Our CEO or other appropriate member of Senior Management is responsible for ensuring annually that our AML program is reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of the Bank Secrecy Act (BSA) and other AML provisions under the USA PATRIOT Act and FINRA, and their implementing regulations.

The designated principal will review our AML program and any reports relating to the testing thereof, as well as any correspondence prepared by our AML Principal concerning the program and any other relevant materials speaking to the strengths and weaknesses of our AML program.

We will maintain all materials reviewed for this purpose in the AML files, and evidence such review by initials and dates. If everything is found acceptable under the current program, the designated principal will obtain written Senior Management approval (see sample language below) and maintain the signed and dated approval in the AML files.

If the review determined the need for some adjustment to our AML program, Senior Management and Compliance will meet with our AML Principal to determine the corrective measures to be taken before the Senior Management approval document can be signed. Our AML files will contain detailed notes on what areas need corrective measures, the reasons it was determined that the corrective measures were required, time frames for putting such corrective measures into effect, the names of the individuals responsible for ensuring corrective measures are followed up on, etc.

AML Principal: ____Jeffrey Ameen__________________________ Date: __3/29/23________

Signature:

SENIOR MANAGEMENT APPROVAL

All Senior Management of Spire Investment Partners are aware of the requirement to have in place an anti-money laundering program under the Bank Secrecy Act, Section 352 of the USA PATRIOT Act, and as required by FINRA Rule 3310

Understanding the serious nature of these requirements and the reasons for which they have been put into place, I, a member of Senior Management, am committed to ensuring that Spire Investment Partners has a program that (a) is effective in light of the nature of our business; (b) is continuously and appropriately overseen; and (c) enhancements are made in any areas found to be deficient in ensuring that we have no customers engaging in money laundering activities.

I have reviewed the current AML program and have found it to be suitable in terms of our efforts to deter and detect any criminal activities that may be attempted through our firm's activities.

I, the undersigned, along with other members of Senior Management, am available at all times to assist any individuals given the responsibility to oversee our anti-money laundering program.

Senior Management is intent on creating an internal environment indicative of our support of all anti-money laundering compliance efforts, as we have done concerning all compliance requirements.

____ Date: ______________

(Signature)

__________Sue McKeown, CCO_____________________________________

(Typed / printed name and appropriate Senior Management title)