

Anti-Money Laundering (AML) Compliance and Supervisory Procedures

Firm Policy

It is the policy of the firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds, so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the “placement” stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler’s checks, or deposited into accounts at financial institutions. At the “layering” stage, the funds are transferred or moved into accounts of other financial institutions to further separate the money from its criminal origin. In the “integration” stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

AML Compliance Contact Designation and Duties

The firm designates Matt Jackson as its Anti-Money Laundering Program Compliance Contact, with full responsibility for the firm’s AML program. The duties of the AML Compliance Contact, notified to FINRA via the FINRA Contact System (Gateway) annually and updated when necessary, will include monitoring the firm’s AML compliance, overseeing communication and training for employees and review of FINRA Rules for any applicable registration requirements. The AML Compliance contact will also ensure that proper AML records are kept. When warranted, the AML Compliance Contact with the approval of a principal of the firm will ensure Suspicious Activity Reports (SARs) are filed. In the absence of the designated compliance contact, all responsibilities will be designated to CCO of the firm, Matt Jackson which is located at 8500 W 110th St Overland Park, KS 66210.

Providing AML Information for the FinCEN 314(a) list

The 314(a) list is a list distributed by FinCEN every other week. Per the Treasury’s final regulations, we will respond to a Financial Crimes Enforcement Network (FinCEN) request about accounts or transactions by immediately searching our records, at our head office or at one of our branches operating in the United States, to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity, or organization named in FinCEN’s request. The 314(a) list is sent to the CCO. Unless otherwise stated in FinCEN’s request, we are required to search current accounts, accounts maintained by a named suspect during

the preceding 12 months, and transactions conducted by or on behalf of or with a named subject during the preceding six months. If we find a match, we will report it to FinCEN by completing FinCEN's subject information form. This form can be sent to FinCEN by electronic mail at sys314a@fincen.treas.gov, or by facsimile transmission to 703-905-3660. If the search parameters differ from those mentioned above we will limit our search accordingly.

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

We will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. We will maintain procedures to protect the security and confidentiality of requests from FinCEN, such as those established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act.

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

We will not use information provided to FinCEN for any purpose other than (1) to report to FinCEN as required under Section 314 of the PATRIOT Act; (2) to determine whether to establish or maintain an account, or to engage in a transaction; or (3) to assist the firm in complying with any requirement of Section 314 of the PATRIOT Act.

Providing AML Information to Federal Law Enforcement Agencies

Per The SAR Review – Trends, Tips, & Issues; Aug 2004, Issue 7 when a financial institution receives a discovery request or a subpoena asking for the production of a SAR, it should contact its primary federal regulator and FinCEN. ISI's primary federal regulator is FINRA. Chapter X of the Department of Treasury's rules and regulations requires banks to notify FinCEN if they receive a subpoena covering SAR.

When any request for a SAR or supporting documentation is presented from its primary federal regulator, law enforcement or any other federal law enforcement agency such as FinCEN, ISI will take all appropriate steps verify the identity of the person requesting the documentation. This may include an independent verification of employment with the requesting entity, visual inspection of physical identification, and any other means available to ISI to satisfy that the requesting person is indeed member of the requesting entity. (Refer to Exhibit 3 - FinCEN guidance "FIN-2007-G003" issued June 13, 2007 for further information.) FinCEN regulations regarding the confidentiality of suspicious activity reports (SARs) require a broker-dealer to make SARs and supporting documentation available to any self-regulatory organization (SRO) that examines the broker-dealer for compliance with the requirements of 31 CFR 1023.320 (the SAR Rule), upon the request of the SEC.1 On January 26, 2012, the SEC issued a letter to FINRA authorizing FINRA staff to ask for SARs and SAR information from member firms in certain circumstances. (Regulatory Notice 12-08)

Providing AML Information to 314(b) registered financial institutions

Registration under 314(b) allows a financial institution or an association of financial institutions to share information with other financial institutions or associations of financial institutions regarding individuals, entities, organizations, and countries for purposes of detecting, identifying, or reporting activities that the financial institution or association suspects may involve possible money laundering or terrorist activities. The list of participating financial institutions is confidential and any subsequent information received from FinCEN regarding participation lists should be treated as such. The lists should not be further disseminated.

The right to share information shall be effective for the one-year period. To continue sharing information after the end of the one-year period, a financial institution or association of financial institutions must submit a new notification form to FinCEN.

I. Voluntary Registration

ISI's participation in the information sharing program under 314(b) is purely voluntary. The Act does not require any financial institution to participate. However, it was determined that ISI should register as a participant in the program .ISI first registered with FinCEN in January 2007 and re-registers annually. The operations manager is responsible to ensure re-registration occurs when required.

II. Registration Process

To complete the annual registration process:

- A. Access FinCEN's website (www.fincen.gov) via the Internet.
- B. From the site menu, select "Section 314(b) Notification"
- C. At the next screen, select "On-line 314(b) Registration"
- D. At the next page, insert CU Investment Solutions LLC as the financial institution being registered.
- E. As you scroll down on that same page, insert the other information as requested. Again, the CCO is the contact person. Other useful information in completing this form: ISI's tax ID #481061886; the primary federal regulator is FINRA.
- F. Once the information is entered, click on the "Send" key to submit the information to FinCEN.
- G. In the next week to two weeks, the contact person will receive an e-mail back from FinCEN acknowledging receipt of the registration. This e-mail should be retained both electronically and in hardcopy.
- H. Following completion of the annual registration, the operations manager will place a tickler on their Outlook calendar as a reminder to renew registration with FinCEN in another year.

III. Changing Point-of-Contact Information

To update ISI's point-of-contact information (individual's name, telephone number, address, e-mail, or fax number), submit an electronic request from your e-mail address of record, as indicated on the 314(b) List of Participants. These requests may be e-mailed to: patriot@fincen.treas.gov. NOTE: Updating point-of-contact information will not change your institution's effective share date.

IV. Use of the 314(b) lists

A. In order to access the electronic version of the 314(b) lists, the point of contact person will have received an e-mail from FinCEN which included a password allowing such authority. With this password, the list can be accessed from the FinCEN website. The password renews each quarter upon e-mail notice from FinCEN.

B. The list contains the names of financial institutions and associations of financial institutions that have notified FinCEN of their intent to voluntarily share information pursuant to Chapter X. Subject to the provisions of this Section, ISI may, under the protection of the safe harbor from liability, transmit, receive, or otherwise share information with any other financial institution or association of financial institutions regarding individuals, entities, organizations, and countries for purposes of identifying and, where appropriate, reporting activities that the financial institution or association suspects may involve possible terrorist activity or money laundering.

C. Prior to sharing information under this Section, ISI will take reasonable steps to verify that the other financial institution or association with which it intends to share information has submitted the requisite 314(b) notice with FinCEN. This verification requirement may be satisfied by confirming that an information-sharing counterpart appears on the 314(b) list provided by FinCEN or by confirming directly with the counterpart that the requisite notice has been filed with FinCEN.

D. Any information shared or obtained in connection with 314(b) will be appropriately safeguarded and held confidential.

Filing of Suspicious Activity Reports

If suspicious activity is suspected as a result of information sharing with another participating financial institution, ISI may need to file a suspicious activity report. The operations manager will consult with the CCO.

Record Retention

The operations manager will retain all electronic messages received from FinCEN regarding ISI registration and access to participant lists. All information relating to 314(b) will be retained for 5 years.

Customer Identification and Verification

This CIP does not directly apply to any existing customers of ISI, including any existing customer seeking to open a new account with ISI, provided that ISI has a reasonable belief that it knows the true identity of that existing customer. This CIP also does not apply to certain new customers of ISI seeking to open a new account with ISI, including (a) any corporate credit union; (b) any natural person credit union, pursuant to tri-party Registered Representative/Independent Contractor Agreement with a corporate credit union; and (c) certain entities regulated by certain federal or state regulators, as determined on a case-by-case basis. This CIP applies to all other new customers of ISI seeking to open a new account with ISI. This CIP also applies to any existing customer seeking to open a new account, but only if ISI does not have a reasonable belief that it knows the true identity of that existing customer. This is provided for the customers ISI may have that would fall under the CIP regulations, and for other regulatory and recordkeeping purposes.

In addition to the information we must collect under FINRA Rules 2010 (Standards of Commercial Honor and Principles of Trade), 2111 (Suitability), and 4510 (Books and Records), we will, at minimum: verify, to the extent reasonable and practicable, the identity of any customer seeking to open an account; maintain records of information used to verify a customer's identity; and check that a customer does not appear on government terrorist lists, such as the list on Treasury's Office of Foreign Assets Control (OFAC) Web Site.

For recordkeeping and other purposes, we will collect the following information for all accounts, if applicable, for any person, entity or organization who is opening a new account or is being granted trading authority over a new or existing account: the name, mailing address, street address of the principal place of business, phone number, tax ID number, type of charter and corporate resolution. ISI limits its customers to institutional clients. We will gather the additional information specified below for each of the following categories of accounts we provide:

Domestic Operating or Commercial Entities- We will collect information sufficient to determine the corporate or business entity's identity, and the authority of its business representative to act on its behalf. Types of qualifying information are discussed throughout this section of the Program.

Institutional Accounts- Institutional accounts often are opened for financially sophisticated customers who trade frequently, in volume, and usually through an intermediary, some of whose AML policies and procedures are sufficient and verifiable. When dealing with an institutional client, we will consider whether it has an AML program and the quality of that program, the length and nature of experience with the institution, and the regulations of the institution instilled by government and other regulatory agencies.

It is ISI policy not to allow participation in the following transactions and account types: Individual Accounts; Non-U.S. Person Accounts; Domestic Trusts; Foreign and Offshore Entities; High Risk and Non-Cooperative Jurisdictions; Senior Foreign Government/Public Officials; Transferred Accounts; Foreign Correspondent and Foreign Shell Accounts.

To insure the listed accounts are not opened, ISI requires a completed account form to be received at the home office, and reviewed by either the AML contact or a principal of the firm, before a trade can be executed.

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, or the information provided cannot be verified, our firm will not open a new account and, after considering the risks involved, consider closing any existing accounts. In either case, our AML Compliance Contact will be notified so that we can determine whether we should report the situation to FinCEN.

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. In verifying customer identity, we will analyze any logical inconsistencies in the information we obtain. We will verify customer identity through documentary evidence, non-documentary evidence, or both. Non-Documentary evidence will only be used if after using documentary evidence, we are still uncertain about the true identity of the customer.

The following documents are appropriate for verifying the identity of institutional clients:

- A certificate of incorporation, a government-issued business license, partnership agreements, any corporate resolutions, or similar documents.

Verification of customer identity through the use of non-documentary evidence may be required if an account is deemed to need enhanced due diligence. We will use the following non-documentary methods of verifying identity:

- Contact the customer after the account has been opened (although we cannot rely solely on customer contact as a mean for verification)
- Obtain financial statements from the customer
- Compare information obtained from customer with information available from a trusted third-party source
- Check references with other financial institutions
- Any other non-documentary means deemed appropriate

We will verify the information at the time new accounts are opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may restrict the types of transactions or dollar amount of transactions

pending verification. We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancy in the identifying information. We will maintain those records for five years after the account has been closed or the customer's trading authority over the account has ended.

Additional CIP information is provided in the Customer Identification Program section of these procedures (Appendix A).

Using Government-Provided Lists of Terrorists and Other Criminals

Prior to opening an account, and on a monthly basis, we will check to ensure that customer does not appear on, lists provided by the government, including, but not limited to Unauthorized Banks, and Treasury's OFAC "specifically Designated Nationals and Blocked Persons" List (SDN List), non- SDN list and any other US Treasury Finance Sanction list and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the US Treasury website. ISI will use the review performed by the operations manager.

<https://public.govdelivery.com/accounts/USTREAS/subscriber/topics?utf8=%E2%9C%93&commit=Finish>

In the event we determine a customer, or someone with or from whom the customer is transacting, is on any US Treasury Finance Sanction List or is from or engaging in transactions with a person or entity located in an embargoed country or region, we will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC. We will also call the OFAC Hotline at 1-800-540-6322.

If a match against the Unauthorized Banks list is made with a customer attempting to execute a transaction with ISI, the transaction or new account form will be rejected. We will contact the Office of the Comptroller of the Currency at 1-800-613-6743, immediately.

Notice to Customers

The firm will provide a notice to customers on the Account Information Form that we are requesting information from them to verify their identities, as required by federal law. This notice is provided on every account form signed by the secretary of the institution opening the account. The notice states: To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person or entity that opens an account with CU Investment Solutions LLC. What this means for you: When you open an account, we will ask for your name, address, date of birth, telephone number, and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents. For new members other than individuals, we will ask you to provide certain corporate entity documents.

Additional Inquiries

We recognize our obligations under suitability and fair dealing requirements to collect

customer identification information. Depending on the nature of the account, we will take the following additional steps, to the extent reasonable and practicable, when we open the account:

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

Supervisory Procedures for Opening Accounts

Our new account opening procedure is modified to collect and use information on the account holder's assets, anticipated transaction activity, and sources of income to detect and deter possible money-laundering and terrorist financing. Registered Representative's will document why an account is opened absent any information required by the firm to open an account.

Monitoring Accounts For Suspicious Activity

ISI will check daily using the Daily Folder reports to manually monitor account activity. The CCO, FinOps or CCO designee will notice any patterns of unusual size, volume, or transaction type. We will look at transactions, including trading and wire transfers, in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual strategy for that customer. The CCO, FinOps or CCO designee will notify the AML Compliance contact in consultation with a principal of the firm and review documentation on each incident; when and how it is carried out. The AML Compliance contact will report suspicious activities to the appropriate authorities by the appropriate time frame. ISI shall file the suspicious activity report no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing a suspicious activity report (SAR). If no suspect was identified on the date of detection of the incident requiring the filing, ISI may delay filing a suspicious activity report for an additional 30 calendar days to identify a suspect. In no case shall reporting be delayed more than 60 calendar days after the date of initial detection of a reportable transaction. Among the information we will use to determine whether to file a SAR are exception reports that include transaction size, location, type, number, and nature of the activity. Our AML Compliance Contact or designee will conduct an appropriate investigation before a SAR is filed. Our monitoring of transactions includes:

- manual monitoring of account activity by various branch, operation or compliance personnel

ISI shall maintain a copy of any suspicious activity report filed and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the suspicious activity report. Supporting documentation shall be identified and maintained by ISI as such, and shall be deemed to have been filed with the suspicious activity report. ISI will make all supporting documentation available to appropriate law enforcement authorities upon request. ISI management shall promptly notify its board of directors, or a committee thereof, of any report filed pursuant to this section. ALL ISI suspicious activity reports are confidential. No information regarding ISI SAR will be disclosed without proper legal representation.

Emergency Notification to the Government by Telephone

When conducting due diligence or opening an account, we will immediately call Federal law enforcement when necessary, and especially in these emergencies: an 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 or any other government list we review; or we have reason to believe the customer is about to use the funds to further an act of terrorism. We will first call the OFAC Hotline at 1-800-540-6322. The other contact numbers we will use are: Financial Institutions Hotline 1-866-556-3974, local U.S. Attorney's Office 1-816-426-3122, and local FBI Office (816) 512-8200.

Red Flags

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

- The customer exhibits unusual concern regarding the firm's compliance with regulatory reporting requirements, particularly with respect to its type of business and assets; is reluctant or refuses to reveal any information concerning the business activities involving the firm; or furnishes unusual or suspect information regarding its business
- A customer wishes to engage in transactions that lack business sense, apparent investment strategy, or are inconsistent with the customer's stated business strategy
- A customer delivers funds for the purpose of purchasing a long-term investment, followed shortly thereafter by a request to liquidate the position and transfer the proceeds out of the account

Responding to Red Flags and Suspicious Activity

When a member of the firm detects any red flag he or she will investigate further under the direction of the AML Compliance Contact. This may include gathering additional information internally or from third party sources, contacting the government, freezing the account, and filing a SAR.

Suspicious Transactions and Bank Secrecy Act (BSA) Reporting

We may file SARs for any account activity conducted or attempted, through our firm involving \$5,000 or more, where we know, suspect, or have reason to suspect: the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise 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 we know, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the transaction; or the transaction involves the use of the firm to facilitate criminal activity.

We may not base our decision on whether to file a SAR solely on whether the transaction falls above a set threshold. We may file a SAR and notify law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities. Securities law violations that are reported to the SEC or an SRO may also be reported promptly to the local U.S. Attorney as appropriate.

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 we will report them to the SEC or SRO.

All SARs will be promptly reported to the Board of Managers and senior management, with a clear reminder of the need to maintain the confidentiality of the SAR.

Currency Transaction Reports (CTR)

Our firm prohibits the receipt of currency and we do not conduct any of the firm's transactions in currency. If we discover currency has been received, we will file with FinCEN CTRs for transactions involving currency that exceed \$10,000. Multiple transactions involving the same tax identification number will be treated as a single transaction if they total more than \$10,000 during any one business day. We file any required CTR electronically following instructions provided at www.fincen.gov.

Currency and Monetary Instrument Transportation Reports (CMIR)

Our firm prohibits the receipt of currency and we do not conduct any of the firm's transactions in currency. If ISI discovers currency has been received, ISI will file CMIR if the firm transports, mail, ships or receives or causes to transport, mail ship or receive monetary instruments of more than \$10,000 at one time in any one business day. This transaction is only applicable to international shipments of currency in and out of the USA. If required, we will use the CMIR form and filing instructions provided at fincen.gov.

Foreign Bank and Financial Accounts Reports (FBAR)

This is not applicable to ISI as ISI has no foreign account holdings. Procedures are in place to prevent the opening of Foreign Bank and Financial Accounts.

Transfer \$3,000 or More under the Joint and Travel Rule

When transferring funds of any amount, ISI will follow FinCEN procedures in documenting the proper identity and account numbers of transmitters and recipients. No transfer of funds is ever completed for individuals or firm that are not clients of ISI.

AML/OFAC Risk Assessment

The purpose of the assessment is to help management better understand the areas of risk exposure, internal controls adopted to mitigate those risks, and decisions made to accept risk. Annually ISI will complete a risk assessment, or contract for such.

The following general items will be reviewed:

- o Assess ISI procedures and controls against requirements of FINRA , NCUA, and OFAC regulations;
- o Evaluate new ISI customer base for the year and product offering against applicable appendices and matrices in the FFIEC Bank Secrecy Act/AML to gauge the quantity of BSA/AML and OFAC risk. Includes a review of each product type, volume of usage, location of members, and interviews with key personnel involved with daily operations and product offerings

- o Complete a FINRA approved Self-Assessment Questionnaire
- o for any risk identified, research, document and evaluate mitigating controls

A written report will be prepared and submitted to the COO for review and approval.

AML Record Keeping

SAR Maintenance and Confidentiality- We will hold SARs and any supporting documentation confidential. We will not inform anyone outside of law enforcement, a regulatory agency or securities regulator about a SAR. We will deny any law enforcement subpoena requests for SARs or SAR information and immediately tell FinCEN of any such subpoena we receive. We will segregate SAR filings and copies of supporting documentation from other firm books and records to avoid disclosing SAR filings. Our AML Compliance Contact will handle all subpoenas or other requests for SARs.

Responsibility for AML Records and SAR Filing- Our AML Compliance Contact will be responsible to ensure that AML records are maintained properly and that SARs are filed as required and kept in a secure and locked location.

Records Required- As part of our AML program, our firm will create and maintain if applicable, SARs, CTRs, CMIRs, FBARs and relevant documentation on customer identity and verification, and funds transfers and transmittals as well as any records related to customers listed on the SDN, Non-SDN and OFAC list. Documents will be kept according to existing BSA and SEC rules.

Clearing/Introducing Firm Relationships

ISI works closely with Southwest Securities to detect money laundering. We will exchange information, records, and data as necessary to comply with AML law. We will share information with our clearing broker about suspicious transactions in order to determine when a SAR should be filed—unless inappropriate to do so if activity is regarding the clearing broker or its employees.

Training Programs

We will develop ongoing employee training under the leadership of the AML Compliance Contact and senior management. Our training will occur on at least an annual basis. It will be based on our firm's size, its customer base, and its resources. Our training will include some of the following but may vary according to previous trainings: how to identify red flags and signs of money laundering that arise during the course of the employee's duties; what to do once suspicious activity is identified; what employees' roles are in the firm's compliance efforts and how to perform them; the firm's record retention policy; and the disciplinary consequences (including civil and criminal penalties) for non-compliance with the PATRIOT Act, OFAC and Bank Secrecy Act. This can vary based on the evaluation of the Corporate Agents and the amount of training provided to them through their respective Corporate Credit Union.

We will develop training for our firm, or contract for it. Delivery of the training may include educational pamphlets, videos, lectures, and explanatory memos. All new employees are required to read the entire AML program. The CCO will contact new employees to discuss the AML program and provide them with training. We will maintain records to show the persons trained the dates, and the subject matter of their training.

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

Independent Testing Program

The designated AML Officer will ensure annual independent testing will be completed. This will typically be contracted to a third party. After the test is completed, the compliance staff will report its findings to the senior management and Board of Managers. All recommendations will be responded to in a timely manner with additional comments, changes in policy, or action plan items or any combination of the three.

Monitoring Employee Conduct and Accounts

We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the AML Compliance Contact. The AML Compliance Contact's accounts will be reviewed by a principal of the firm.

Confidential Reporting of AML Non-Compliance

Employees will report any violations of the firm's AML compliance program to the AML Compliance Contact, unless the violations implicate the Compliance Contact, in which case the employee shall report to a member of the Board. Such reports will be confidential, and the employee will suffer no retaliation for making them. All alleged violations will be investigated and reported to appropriate authorities if applicable.

Bank Secrecy Act

See Exhibit N for BSA and Policies regarding BSA

Anti-Money Laundering Contact Information

ISI is required to disseminate information on whom to contact for Anti-Money Laundering questions or issues. The following individual may be reached at (913) 912-5240.

Matt Jackson, ext. 235
mjackson@cu-isi.org
8500 W 110th St. #650
Overland Park, KS 66210

Chief Compliance Officer

Senior Management Approval

I have reviewed and approved this Anti-Money Laundering Program as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of Rule 3310, Anti-Money Laundering.

Hard Copy of Approval on File

Signed: _____

Date: _____

By: Matt Jackson

Title: Chief Compliance Officer

