PRIVATE CLIENT SERVICES™

MEMBER FINRA, SIPC
A Registered Investment Advisor

PRIVATE CLIENT SERVICES
ANTI-MONEY LAUNDERING
PROCEDURES

Updated 08/19/2019

Table of Contents

ANTI-MONEY LAUNDERING (AML) PROGRAM: OVERVIEW

Designated Supervising Principal

Anti-money laundering efforts are the responsibility of all associated individuals, from Senior Management to sales assistants. Our AML Principal is responsible for ensuring that our AML Program is appropriate for our business, is monitored, reviewed, tested and amended as required, and that we maintain appropriate documentation evidencing such efforts.

Supervisory Review Procedures and Documentation

This broker-dealer is committed to fostering a company-wide dedication to detect and deter any money laundering or other activity that could facilitate money laundering or the funding of terrorist or criminal activities.

Through our anti-money laundering training program, we ensure that all appropriate registered and non-registered individuals are fully aware of what money laundering is.

Such training discusses, among other things, that 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. Training also discusses the three stages of money laundering: *placement, layering and integration.* Emphasis is placed on the *layering* stage, as this is where we feel we may be at risk. As we do not accept cash or cash equivalents, *placement* is a minimal risk and the *integration* stage would be past the point of deterrence, so while those areas are included in our AML training, l*ayering* is our major area of focus.

In addition, our training discusses the fact that while terrorist financing may not involve the proceeds of criminal conduct, it could be an attempt to conceal the origin or intended use of the funds that could later be used for criminal purposes. This type of activity falls under the USA PATRIOT Act and the ensuing FINRA rules that govern our anti-money laundering policies and procedures.

All registered and appropriate non-registered personnel will receive our policy against money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities in clearly stated language. Senior Management vigorously 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) suspicious activities.

It is the responsibility of Senior Management, all supervising principals and all registered representatives, as well as non-registered individuals (i.e., surveillance, etc.), to act as a team in guarding the firm against being utilized in any manner by money launderers, as the consequences of non-compliance (including significant criminal, civil and disciplinary penalties) are severe.

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

In putting together our anti-money laundering program, our AML Principal and other appropriate individuals have referred to NASD Special Notice to Members 02-21 to ensure that we are utilizing the guidance therein.

Regulatory Reference

NASD Special Notice to Members 02-21

ANTI-MONEY LAUNDERING (AML) PROGRAM: Additional Areas of Risk

Designated Supervising Principal

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, 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.

Supervisory Review Procedures and Documentation

The AML Principal and/or other members of Senior Management will maintain documentation of this review, indicating the individuals involved, dates, findings, etc. If changes to our AML Program are required, the changes will be made and appropriately disseminated. We will maintain documentation of our findings, changes and dissemination lists in the files. Conversely, if a determination is made that the program is sufficient as is, we will document this in our files, evidencing who was involved in making the determination, dates, etc.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Bank Secrecy Regulations - Special Measures

Designated Supervising Principal

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

Supervisory Review Procedures and Documentation

When opening a new customer account for a foreign financial institution, our AML Principal will provide a "One-Time Notification" when applicable informing the representative of record on the account 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, restricted foreign financial banks, 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 restricted foreign bank, 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, 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 restricted foreign bank. 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.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Checking of OFAC and Other Government Lists

Designated Supervising Principal

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.

Supervisory Review Procedures and Documentation

When opening a domestic or foreign account, and on an ongoing basis, 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 AML Principal will ensure that we maintain documentation evidencing that such a check was conducted, how it was conducted, by whom, the date and any other information relevant to the check in terms of possible matches and further investigations.

Our AML Principal will also ensure that existing accounts are reviewed against these lists when they are updated, and retain documentation of when, how and by whom such reviews were undertaken, along with any findings and follow-up activities.

PCS utilizes Artisan Software (Maestro) to complete all OFAC checks for both new and existing accounts. Updates to the SDN lists are received by both the CCO and COO via email notification and are then downloaded from the OFAC site and uploaded into Maestro. The Maestro system records the date of the initial OFAC screening as well as the latest screening date. All accounts are screened versus the uploaded data each time a new list is processed through the system.

In the event that an OFAC check or a check of any other utilized list, leads to a determination that a customer, or someone with or for whom the customer is transacting business, 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 Principal will ensure that such forms are filed within 10 days of determining that a customer is on the SDN list or is engaging in transactions that are prohibited by economic sanction and embargoes. All information relating to such findings will be documented in detailed fashion, and retained in our files. In such instances, the AML Principal will also ensure that we notify OFAC by calling its hotline at 1-800-540-6322.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Clearing Firm Relationship

Designated Supervising Principal

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

Supervisory Review Procedures and Documentation

We will update and maintain documentation on any information exchanged (records, data and exception reports as necessary to comply with AML laws, etc.) including the required annual notices for such information sharing. The designated principal will document this review, 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 4311 (formerly NASD Rule 3230).

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 (indicating by initials and dates any required reviews and follow-up actions taken). 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.

Regulatory Reference

FINRA Rule 4311

ANTI-MONEY LAUNDERING (AML) PROGRAM: Closing Account after Failure to Verify Customer Identity

Designated Supervising Principal

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

Supervisory Review Procedures and Documentation

Any accounts permitted to be opened without the customer's identity fully verified will result in our limiting the terms of the account.

Only an appropriate supervising principal can permit an account to remain open in instances where we have not effectively verified customer identity. We will indicate in notes to the file the name of the individual who determined the account could remain open, the date and any limitations placed on the account. The files will also state the length of time the account may continue to function under the limitations before requiring final customer identity verification.

A list of all such accounts, with the deadline for achieving full customer identification verification, will be maintained by; appropriate supervising principals, our AML Principal and appropriate operations and/or surveillance personnel.

Each of these individuals retains a responsibility to ensure that the account is either fully opened or closed by the deadline, and will maintain documentation in the files about all efforts undertaken and the results and rationale for final decisions made regarding the account.

Our AML Principal has the ultimate responsibility to ensure the constant monitoring of these accounts, to satisfy the requirements to fully open or to close the account, and to maintain appropriate documentation.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Compliance Officer Contact Information

Background

FINRA Rule 3310 requires that each member firm provide to FINRA 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.

Designated Supervising Principal

Our CCO ensures that current contact information is provided to FINRA as required under Rule 3310.

Supervisory Review Procedures and Documentation

Our CCO must ensure that FINRA is initially provided with the following information as it relates to the individual responsible for such activities, and that the information remains current at all times:

- Name of our AML Principal
- Title
- Mailing address
- E-mail address
- Telephone number
- Facsimile (Fax) number

This information is entered into the FINRA Contact System (FCS) in the FINRA website, (http://www.finra.org and then clicking on Regulatory Systems.)

The information maintained on the FCS must be reviewed at least annually to ensure that the information is current and correct. We will maintain documentation of such reviews, evidenced by initials and dates. If any changes are required to the FCS information, we will maintain documentation indicating the revised filings.

Any change in the individual designated as our AML Principal must 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.

Regulatory Reference

FINRA Rule 3310

ANTI-MONEY LAUNDERING (AML) PROGRAM: Compliance Officer Designation and Duties

Designated Supervising Principal

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

Supervisory Review Procedures and Documentation

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

The AML Principal has been named based on his/her experience, knowledge and ongoing continuing education efforts (through reading materials, website resources and general review of all AML rules, training, regulations and requirements). We retain documentation of this individual's qualifications as our AML Principal in the files.

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 broker-dealer to all appropriate individuals
- Diligent monitoring of appropriate websites to remain current with all AML program requirements
- Prompt filing of Currency Transaction Reports (CTRs), should it be determined that cash has been received despite our strict prohibition against receipt of cash
- Prompt filing of Currency and Monetary Instrument Transportation Reports (CMIRs), should it be determined that cash equivalents or other monetary instruments not approved for receipt, such as cashier's checks, bearer bonds, travelers checks, etc., have been received despite our strict prohibition against the receipt of such items
- Annual filing of Foreign Bank and Financial Reports (FBARs), for foreign accounts held in the name of this broker-dealer
- 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 completed 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 requisite time frames to all governmental and regulatory agencies for information concerning any accounts we may hold
- Maintaining records concerning the above and any other AML activities, for a minimum five year period after account closing

Our AML Principal will ensure that records relating to all of the above, and any other AML efforts, are maintained to document, by signed and dated notes to the files, the manner and extent of our compliance in each area.

Periodically, our AML Principal may oversee the testing of our AML procedures to determine whether all of our AML procedures and requirements are appropriately undertaken and documented. Our AML Principal will maintain documentation of all review findings, including any remedial steps taken when required.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Confidential Reporting by Employees of AML Non-Compliance

Designated Supervising Principal

Designated Supervisors, Senior Management and our AML Principal will endeavor to ensure that all employees are made aware of the requirement under FINRA Rule 3310 to immediately disclose any detected or perceived AML violations.

Supervisory Review Procedures and Documentation

Our AML training, as well as discussions during our Annual Compliance Meeting and by other manners as deemed appropriate, may include various topics as appropriate, including informing 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.

It is the policy of Private Client Services that any reports will remain confidential and that the reporting individual will suffer no retaliation or consequences for making the report.

We will maintain documentation regarding this employee training, indicating manner of training, dates, names of individuals conducting the training, and lists of individuals who received the training.

Regulatory Reference

FINRA Rule 3310

ANTI-MONEY LAUNDERING (AML) PROGRAM: Credit Extensions

Background

Our AML Principal must ensure that, if and when applicable, we maintain appropriate AML records for all extensions of credit.

Supervisory Review Procedures and Documentation

We do not currently extend credit to any customers outside of the use of margin loans within a brokerage account custodied by Pershing, LLC or TD Ameritrade.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Currency and Monetary Instrument Transportation Reports (CMIRs)

Background

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.

Designated Supervising Principal

Our AML Principal will ensure that all CMIRs are filed when required.

Supervisory Review Procedures and Documentation

Regardless of whether we permit the receipt of currency, we must have procedures in place either to monitor our prohibition, filing CMIRs only when such prohibition has been violated, or to routinely review for CMIR filing requirements based on receipt of currency. We will maintain documentation of all review activities to ensure detection of currency acceptance, or to determine which had required CMIR filings. We will retain documentation in our files, indicating by initials and dates, which documents were reviewed and what findings resulted.

If it is discovered that currency has been received, our AML Principal is responsible for filing a CMIR with the Commissioner of Customs - that is, whenever the firm transports, mails, ships or receives or causes or attempts to transport, mail, ship or receive monetary instruments of more than $10,000 at one time, on one calendar day or, if for the purpose of evading the reporting requirements, on one or more days, in or out of the U.S. We

will maintain copies of all such filings in our files.

A CMIR is required for all such shipments or receipts of monetary instruments, except for currency or monetary instruments shipped or mailed through the postal service or by common carrier. We will, however, file a CMIR for such receipts of currency and monetary instruments and for shipments and deliveries made by the firm by means other than the postal service or common carrier, even when such shipment or transport is made by the firm to an office of the firm located outside the U.S.

Our AML Principal will ensure that should we need to file a CMIT, we will do so electronically, by first registering with FinCEN by logging onto http://bsaefiling.fincen.treas.gov.

Where a CMIR must be filed because an individual violated our prohibition against accepting currency, the individual will face serious sanctions, including the likely possibility of termination. We will maintain documentation of all investigations concerning such violations including the rationale for final sanctions put into effect, in our files.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Currency Transaction Reports (CTRs)

Background

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.

Designated Supervising Principal

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

Supervisory Review Procedures and Documentation

This broker-dealer 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. We will maintain documentation indicating training dates, materials utilized, and lists of the individuals who receive such training, etc., in our files.
- 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).
- In instances where currency was received despite our prohibition, the circumstances will be investigated and the individual involved will face sanctions, including the possibility of termination.

ANTI-MONEY LAUNDERING (AML) PROGRAM: 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).

FinCEN, the bureau of the Department of the Treasury responsible for administering the BSA and its implementing regulations, issued the CDD Rule to clarify and strengthen customer due diligence for covered financial institutions, including broker-dealers.

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; and (4) ongoing monitoring for reporting suspicious transactions and, on a risk basis, maintaining and updating customer information. As the first component is already an AML program requirement, 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 identify and verify the identity of the beneficial owners of all legal entity customers at the time a new account is opened, subject to certain exclusions and exemptions. 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."

FinCEN's CDD Rule does not change the requirements of FINRA Rule 3310, and member firms must continue to comply with its requirements. However, FinCEN's CDD Rule amends the minimum statutory requirements for member firms' AML programs by requiring such programs to include risk-based procedures for conducting ongoing customer due diligence. This ongoing customer due diligence element, or "fifth pillar" required for AML programs, includes: (1) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and (2) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information. As stated in the CDD Rule, these provisions are not new and merely codify existing expectations for firms to adequately identify and report suspicious transactions as required under the BSA and encapsulate practices generally undertaken already by securities firms to know and understand their customers.

Designated Supervising Principal

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.

Supervisory Review Procedures and Documentation

We have established new account opening procedures that require our associated personnel to collect and use information on the account holder or beneficial owner's identity, employment, past history, wealth, net worth, anticipated transaction activity and sources of income, to detect and deter possible money laundering and terrorist financing.

Under the FinCEN CDD Rule, account opening procedures for corporations now require us to look through and document the identity of beneficial owners. There are both ownership and control prongs of the definition of beneficial owner for purposes of the CDD Rule. A beneficial owner is: (1) each individual (if any) who directly or indirectly owns 25 percent of the equity interests of a legal entity customer; and (2) a single individual with significant responsibility to control, manage, or direct a legal entity customer, including an executive officer or senior manager.

PRIOR to opening an account, we must minimally obtain for account or beneficial owners:

- A name
- Date of Birth
- For an individual, a residential or business street address
- For an individual who does not have a residential or business street address, an APO or FPO box number or business street address of a next of kin or other contact individual
- For other than an individual (i.e., corporation, partnership, trust, etc.), a principal place of business, local office or other physical location
- An identification number
- For a US person, a taxpayer identification number (Social Security Number or employer identification number)
- For a non-US person, one or more of the following:
    - A taxpayer identification number (TIN)
    - 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

In addition, we must have an understanding of the nature and purpose of the customer relationship in order to determine whether a transaction is potentially suspicious in order to fulfill suspicious reporting obligations and to develop a customer risk profile.

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

Given proof that a natural or non-natural customer has applied for, but has not yet received, a taxpayer identification number, our CIP program allows the account to be opened, as 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 taxpayer identification numbers during the period of time the account is open prior to receipt of such numbers.

Our policy is that all such accounts will be closed within 30 days if the taxpayer identification number is not received. Exceptions to this policy may only be made if approved by our AML Principal, documented by initials and date on the new account form. In addition, a note must be made to the file, signed by our AML Principal,

indicating why such an extension was granted and the period of time for which the extension is in place. When the extension time limit has expired, we will adhere to the same procedures as in the first instance of allowing such an account to be opened.

Registered personnel are encouraged, through AML training, Annual Compliance Meetings and other compliance-related training, to make every effort to obtain more than one type of documentary verification. The more information we obtain regarding our customers, the greater the likelihood that we would find inconsistencies in instances when a person is attempting to provide false, or less than complete, information.

In addition, and most specifically 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. In instances where 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 determined to exist.

Another 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 low-risk instances, supervising principals at the time of the account opening, or our AML principal at the time of review, may require some non-documented verification to back up the documented verification.

Documentary verification is required as follows: Individual including beneficial owners

- Unexpired government-issued ID evidencing nationality or residency and bearing a photograph or similar safeguard (e.g., 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 we know the true identity of the customer

Non-Individual (although beneficial owners as defined above still need to be verified)

- 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 may include, but are not necessarily limited to:

- Contacting the customer
- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source. Compare information obtained from the customer against databases such as Equifax, Experian, Lexis/Nexis, or other in-house or custom databases.)
- 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 Social Security Number). For example, does the zip code match the city/state? Is the area code given appropriate for the address? Does date of birth reflect the individual's appearance?

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

- When the customer is unable to present an unexpired government-issued identification document with a

photograph or other similar safeguard
- When the firm is unfamiliar with the documents the customer presents for identification verification
- When the customer and firm do not have face-to-face contact
- When other circumstances 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 an effective AML Program, our AML Principal, in conjunction with other Senior Management and compliance personnel, have 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 methods and by adhering to the minimal requirements set forth in the USA PATRIOT Act, occasionally the risk of not knowing the customer sufficiently may be heightened for certain accounts.

For those customers identified as having heightened risk, we require that the identification go beyond the customer.

Type of accounts that 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 U.S. as a primary money laundering haven, or that have been designated as non-cooperative by an international body
- Corporations, trusts, and partnerships conducting substantial business in a jurisdiction that has been designated by the U.S. as a primary money laundering haven or has 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. (i.e. at minimum, those with 25 percent ownership)

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

- Inquire about the source of the customer's assets and income to determine whether 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 to detect any deviations from the patterns at a later date.

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

Regulatory Reference

Section 326 of the USA PATRIOT Act

ANTI-MONEY LAUNDERING (AML) PROGRAM: Customer Notification

Designated Supervising Principal

Our AML Principal ensures that all customer notification as required under FINRA Rule 3310 is appropriately delivered.

Supervisory Review Procedures and Documentation

Prior to opening an account, notice must be given to the customer indicating that we are requesting information to verify their identity. Depending on how we open accounts, we may give such notice:

- On our web site
- With account applications
- Any other means of written

All registered representatives and supervisory personnel will be advised how we are making this notification, the specific language to be utilized and how to access copies of the notice (with evidence of such training maintained in the files).

On not less than an annual basis, our AML Principal will review the manner in which we make customer notification, test to ensure that it is appropriately made and determine if new procedures need to be put into place. Documentation as to each such review, including any findings and remedial actions taken, if necessary, will be maintained in the files.

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.

At the time of account opening, we are required to collect information such as the following from each customer:

- Name
- Date of birth
- 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.

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 require a customer to provide most of this information. These rules also may require additional information, such as net worth, annual income, occupation, employment information, investment experience and objectives, and risk tolerance.

Regulatory Reference
FINRA Rule 3310

ANTI-MONEY LAUNDERING (AML) PROGRAM: Customers Who Refuse to Provide Information

Designated Supervising Principal

Our AML Principal ensures that all registered personnel appropriately handle account openings when faced with customers who refuse to provide the required information. In addition, each individual's immediate

supervising principal is responsible for ongoing oversight to ensure these situations are handled according to the rules and regulations as well as with our internal policies and procedures.

Supervisory Review Procedures and Documentation

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

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, initialing and dating all documents reviewed.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Denying Accounts

Designated Supervising Principal

Our AML Principal will ensure that all registered personnel appropriately handle account openings when faced with a potential money laundering concern that may require us to deny opening the account. In addition, each individual's immediate supervising principal is responsible for ongoing oversight to ensure these situations are handled according to the rules and regulations as well as with our internal policies and procedures.

Supervisory Review Procedures and Documentation

We will deny opening accounts in certain suspect jurisdictions for which we cannot obtain sufficient information, both for the account holder and/or for appropriate associated individuals that we determine carry too much risk.

We will deny requests to open accounts for those who appear overly reluctant to supply us with requisite information simply due to the lack of sufficient information and lack of cooperation.

We will deny requests to open accounts for which it appears that we know the customer, but questions about the specific source of wealth were not easily addressed.

We will deny requests to open accounts that, for whatever reason, we are not comfortable opening and for which we have been unable to obtain sufficient information to eliminate that discomfort.

We will maintain documentation about all denied accounts, indicating why the account was denied and whether a determination was made to either file a Suspicious Activity Report (SAR) or to alert authorities, and documentation regarding any other action taken regarding these accounts. Documentation will be initialed and dated, indicating the review of specific documents.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Emergency Telephone Notification to the Government

Designated Supervising Principal

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.

Supervisory Review Procedures and Documentation

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

- Financial Institutions Hotline (1-866-556-3974)
- Local U.S. Attorney's Office
- Local FBI Office
- Local SEC Office

Suspicious Activity Reports (SAR) 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 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.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Filing a Suspicious Activity Report (SAR)

Designated Supervising Principal

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

Supervisory Review Procedures and Documentation

SAR-SF filings are required under the Bank Secrecy Act (BSA) for any account activity (including deposits and transfers) 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
- The transaction involves the use of the firm to facilitate criminal activity

Our AML Principal will ensure that decisions whether to file SAR-SFs are not based solely on whether transactions fall above a set threshold. We will file a SAR-SF and notify law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities.

In high-risk situations, we will notify the appropriate government agency immediately and file an SAR-SF 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-SF 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 an SAR-SF, as well as a copy of the filing.

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

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

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

Our AML Principal will become familiar with available resources such as FinCEN's website which contains additional information including annual SAR-SF Activity Reviews and SAR-SF Bulletins that discuss tips and trends in suspicious reporting.

SAR-SF instructions are available on FinCEN's website at http://www.fincen.gov/fin101_instructions_only.pdf

ANTI-MONEY LAUNDERING (AML) PROGRAM: Foreign Bank and Financial Accounts Reports (FBARs)

Designated Supervising Principal

Our AML Principal will ensure that, if applicable, annual FBARs are appropriately filed.

Supervisory Review Procedures and Documentation

Our AML Principal will ensure that we submit a Foreign Bank and Financial Account Form (Form TD F 90-22.1 or FBAR) for any accounts that this broker-dealer has a financial interest in, or signature authority over, a financial account held anywhere outside the U.S. that entails more than $10,000, as required under Exchange Act Rule 17a-8 and the Bank Secrecy Act. This FBAR must be filed on an annual basis no later than June 30.

Annually, and in a manner sufficiently timed to meet the June 30 FinCEN filing deadline, our AML Principal will request that Senior Management complete a form requesting information about any foreign accounts in which this firm has a financial interest or signature authority over.

We will maintain documentation indicating the request from Senior Management and any follow-up steps taken regarding FBAR filings as part of our AML books and records.

Regulatory Reference

Exchange Act Rule 17a-8

ANTI-MONEY LAUNDERING (AML) PROGRAM: Foreign Correspondent Accounts and Foreign Shell Banks

Background

Broker-dealers are prohibited from maintaining correspondent accounts for unregulated foreign shell banks. "Foreign shell banks" are foreign banks without a physical presence in any country. The prohibition does not include foreign shell banks that are affiliates of a depository institution, credit union or foreign bank that maintains a physical presence in the U.S. or a foreign country and are subject to supervision by a banking authority in the country regulating that affiliated depository institution, credit union or foreign bank.

Designated Supervising Principal

Our AML Principal ensures that all registered personnel appropriately handle foreign bank account openings. In addition, each individual's immediate supervising principal is responsible for ongoing oversight to ensure these situations are handled according to the rules, regulations and our internal policies and procedures.

Supervisory Review Procedures and Documentation

We will detect correspondent accounts (any account that permits the foreign financial institution to engage in securities or futures transactions, funds transfers or other types of financial transactions) for unregulated foreign shell banks by reviewing all account titles not less than annually, looking for key words such as bank, financial or other typical words utilized by a banking institution.

Upon finding, or suspecting such accounts to be foreign banking institutions, we will investigate to determine whether such account should be closed or whether we have appropriate documentation to indicate that the account is not a foreign shell bank. We will maintain documentation regarding all such investigations, evidencing documents reviewed by initials and dates, along with the results and follow-up actions taken, where necessary.

Any accounts for which we do not have appropriate documentation to prove they are not shell banks will be frozen until such time as we have received back from the client the approved certification form and the name and address of a U.S. resident to receive all Service of Process filings. We will maintain documentation of all such frozen accounts, including the date of the freezing and indications of when the certification form was sent and all required information requested, in our files.

Accounts for which we do not receive an acceptable certification form and U.S. resident's name will be closed within 30 days of the request for information, as will any correspondent account that we determine is not maintained by an unregulated foreign shell bank but is being used to provide services to such a shell bank. We will exercise caution regarding liquidating positions in such accounts and take reasonable steps to ensure that no new positions are established in these accounts during the termination period. We will maintain documentation about all such actions, evidencing all review activities by initials and dates, including all follow-up steps taken with dates and appropriate correspondence, as part of our AML books and records.

The 30-day timeframe for closing any accounts for which we have not obtained the information required for bank customers may be extended SOLELY by the signed and dated approval of our AML Principal in instances where it is shown that we are in touch with the customer and have been assured that the information is being gathered for us.

Our AML Principal must ensure that we monitor and adhere to all requirements covering bank and correspondent accounts and that all supervising principals and registered employees are aware of the requirements (i.e., through training, Annual Compliance Meetings, etc.). We will maintain documentation regarding all such training, indicating dates, attendees, agendas, handout materials, etc., in our AML files. We will also maintain evidence of our monitoring.

Mandatory Enhanced Due Diligence

Our AML Principal is responsible for determining whether any foreign correspondent account is maintained for a foreign bank that operates under offshore banking licenses or under a banking license issued by certain jurisdictions specified in 31 C.F.R. §103.176 (c).

For such correspondent accounts, we will apply the enhanced due diligence requirements of 31 C.F.R. §103.176 (b), which include enhanced scrutiny, a determination whether the foreign bank maintains its own correspondent accounts for other foreign banks and identification of certain owners of the foreign bank. This enhanced scrutiny will include obtaining and reviewing documentation from the foreign bank about its own AML program and evaluating the effectiveness of this AML program at detecting and preventing money laundering. In our AML files, we will maintain documentation for all accounts under enhanced due diligence, including requests for information, discussions with the individuals servicing the accounts, etc.

If deemed appropriate by the parties involved (e.g., registered representative, supervising principal and/or our AML Principal), the enhanced scrutiny may also include closer monitoring of account activity, obtaining information about sources and beneficial ownership of funds and identifying persons with trading authority. Depending upon what information we receive as a result of these enhanced due diligence steps, we may be required to gather even more information. We will retain documentation in our AML files, including information related to the foregoing information requirements, indicating who was responsible for obtaining the information, what was requested, dates requested, dates received, etc.

If at some point we determine that we cannot adequately perform due diligence, our AML Principal will make a decision whether to

- Not permit the account to be opened
- Suspend the transaction activity
- File a Suspicious Activity Report (SAR) and contact FinCEN for instructions on how to deal with the account

We will maintain documentation about all due diligence steps undertaken and rationale for any final decision as part of our AML books and records.

Exception for Federal Reserve Designated Jurisdictions

We will not automatically apply these enhanced due diligence procedures for foreign banks operating under offshore branch licenses if the bank is located or chartered in a jurisdiction that has been found by the Federal Reserve to be subject to comprehensive supervision or regulation on a consolidated basis by relevant supervisors in that jurisdiction, provided that the jurisdiction is not on the Financial Action Task Force (FATF) list or Treasury's list of jurisdictions requiring special measures. Instead, we will follow the risk-based assessment specified below to determine whether any enhanced scrutiny is appropriate.

Enhanced Due Diligence Resulting from Risk-Based Assessments

Our AML Principal and other appropriate individuals will make a risk-based assessment about whether any foreign correspondent account poses a significant risk of money laundering activity, taking into account the foreign financial institution's lines of business, size, customer base, location, products and services offered, nature of the correspondent account and the type of transactions for which the account will be used, based on our level of comfort about the entity and individuals involved.

We will also consider any guidance issued by the U.S. Treasury, the SEC, any other government agency or FINRA regarding money laundering risks associated with particular foreign financial institutions and types of correspondent accounts, as well as any public information on whether our customers have been the subject of criminal action of any kind or any regulatory action relating to money laundering.

If we determine that an account poses a significant risk of money laundering activity, we will

- Freeze the account
- File a SAR
- Make an emergency call to FinCEN
- Follow FinCEN instructions for further action

By undertaking an annual review and documenting the results of that review in our AML files, our CCO will also ensure that we are taking steps to determine where enhanced due diligence steps are required in deciding whether to accept a foreign correspondent account. Such steps include:

- Determining whether the account is subject to enhanced due diligence requirements under Section 103.176(b) of the USA PATRIOT Act
- Assessing whether the foreign financial institution presents a significant risk for money laundering
- Considering information available from U.S. government agencies and multinational organizations with respect to supervision and regulation, applicable to the foreign financial institution
- Reviewing guidance from federal agencies or regulators regarding money laundering risks associated with particular foreign financial institutions and correspondent accounts for foreign financial institutions
- Reviewing public information to ascertain whether the foreign financial institution has been the subject of criminal action of any nature or regulatory action relating to money laundering

Recordkeeping for Foreign Correspondent Accounts

Firms must keep records identifying the owners of foreign banks with U.S. correspondent accounts and the name and address of the U.S. agent for service of legal process for those banks. Using Treasury forms to collect the information provides us with a safe harbor.

As indicated previously, our AML Principal is responsible for requiring our foreign bank account holders to complete model certifications issued by the Treasury. We will send the certification forms to our foreign bank account holders for completion, which includes certification that they are not shell banks and provides ownership and agent information.

Our AML Principal is also responsible for overseeing recertification required (a) when we believe for any reason that the information is no longer accurate and (b) at least every three (3) years. We will retain all correspondence regarding such certification efforts.

We will close any account within 10 days of learning from Treasury or the Department of Justice that the bank has failed to comply with a summons or has contested a summons or has not responded to our request for certification and additional information.

During the 10-day period between hearing from Treasury or the Department of Justice and closing the account, under the supervision of our AML Principal we will scrutinize all account activity to ensure that any suspicious activity is appropriately reported and that no new positions are established in these accounts. Our AML Principal is responsible for this period of continuous scrutiny and for retaining records concerning all relevant activities and information.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Freezing of Accounts

Designated Supervising Principal

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

Supervisory Review Procedures and Documentation

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.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Giving Information to Federal Law Enforcement Agencies and Other Financial Institutions

Background

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 addresses law enforcement requests for the production of domestic and foreign bank records. All such requests must be responded to within seven (7) calendar days.

Designated Supervising Principal

Our AML Principal ensures that all requests received from federal law enforcement agencies or other financial institutions are responded to in a timely manner as required under FinCEN/Law Enforcement Requests and USA PATRIOT Act Sections 314 and 319.

Supervisory Review Procedures and Documentation

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

As required under USA PATRIOT Act Section 314, our AML Principal will ensure that we respond to all FinCEN requests for information about accounts or transactions by reporting to FinCEN 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 (via FinCEN's Web-based 314(a) Secure Information Sharing System) to FinCEN as soon as possible but no later than two weeks 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 ensure that our search of FinCEN's 314(a) requests is structured appropriately, based on FinCEN instructions and guidance.

For Section 319 requests which address the production of domestic and foreign bank records, we will respond to the requesting law enforcement authority within seven days.

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 either 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 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.

Regulatory Reference

USA PATRIOT Act Section 314

ANTI-MONEY LAUNDERING (AML) PROGRAM: Grand Jury Subpoenas

Designated Supervising Principal

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

Supervisory Review Procedures and Documentation

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 determined to be suspicious. Should such a finding be made, a SAR will be filed.

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 as a result of an investigation undertaken due to the receipt of 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.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Handling of Accounts for Which SAR Has Been Filed

Designated Supervising Principal

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.

Supervisory Review Procedures and Documentation

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-SF filed. All such accounts must be:

- Permanently closed, or
- Temporarily frozen, or

- Limited in activity, or
- Monitored daily pending final determination

Periodically, we may review all SAR-SF 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.

ANTI-MONEY LAUNDERING (AML) PROGRAM: High Risk and Non-Cooperative Jurisdictions

Designated Supervising Principal

Our AML Principal will ensure that all appropriate registered personnel receive 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.

Supervisory Review Procedures and Documentation

All accounts located in problematic countries will be carefully scrutinized, and we will maintain documentation in the file evidencing such scrutiny.

We will 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. We will maintain records of the rationale for our actions.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Lack of Belief that True Identity of Customer Is Known

Designated Supervising Principal

Our AML Principal will ensure that all registered personnel deal appropriately with those accounts for which we are not reasonably certain of the true identity of the customer.

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

Supervisory Review Procedures and Documentation

When personnel, including the registered representative, the supervising principal approving the account, the Compliance Department, our AML Principal and/or Senior Management, are concerned that we do not sufficiently know the customer, the following options, which are not necessarily mutually exclusive, are available.

- Deny opening the account
- Open the account but limit its terms while continuing to attempt to verify the customer's identity
- Close the account after attempts to verify a customer's identity have failed
- File a SAR

We will maintain documentation in our AML files of all training on how to ensure that a customer is known to

us and subsequent steps, indicating the training dates, hand-out material if appropriate, lists of individuals completing the training, etc.

We will also maintain documentation concerning any accounts where we determined that we did not know the customer, including the rationale for the follow-up action taken.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Limiting the Terms of an Account

Designated Supervising Principal

Our AML Principal will ensure that all registered personnel deal appropriately with those accounts for which we are not able to be reasonably certain of the true identity of the customer.

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

Supervisory Review Procedures and Documentation

In certain instances, accounts that our AML Principal have approved in writing may be opened for a limited period. These accounts will be carefully monitored and will be limited in terms of activities.

Depending upon the nature of the account, the intensions of the account holder and other issues, the limitations placed on the account will be stated to the customer, the registered representative, the appropriate supervising principal and appropriate operations and surveillance personnel. We will maintain documentation of such communications in the files.

We will also document the limitations in writing, signed by the AML Principal, and retain this information in the client file. A time frame for all limitations on such accounts will be indicated, with further action taken (i.e., removal of the limitations or closing of the account and/or the possible filing of a Suspicious Activity Report-SF (SAR-SF)) also documented.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Monitoring Accounts for Suspicious Activity

Designated Supervising Principal

Designated Supervising Principals, Operations and our AML Principal, will endeavor to ensure that all accounts are appropriately monitored to detect suspicious activity.

Each individual's immediate Supervising Principal is responsible for daily supervision to ensure these situations are handled according to the rules and regulations, as well as with our internal policies and procedures.

Supervisory Review Procedures and Documentation

When securities are undertaken through partnership with a clearing firm, we will typically conduct our monitoring through the automated means of exception reports for unusual size, volume, pattern or type of transactions. Our AML Principal works with our clearing firm to ensure that all appropriate exception reports are made available to us and to request the design of additional reports if we are unable to adequately monitor without further information. We endeavor to maintain documentation concerning the exception reports we utilize, dates of such utilization, initials of the individuals undertaking the exception report review, and any findings and follow-up actions, as part of our AML books and records.

For securities transactions not sent through a clearing firm, we may manually monitor a sufficient amount of account activity to permit identification of patterns of unusual size, volume, pattern or type of transactions,

geographic factors such as whether jurisdictions designated as non-cooperative are involved, or any identified red flags. Market manipulation, pre-arranged or other non-competitive trading, or wash or other fictitious trading is strictly prohibited.

Our AML Principal will create the monitoring parameters, minimally including trading and wire transfers, in the context of other account activity to determine whether a transaction lacks financial sense or is suspicious because it is an unusual strategy for that customer.

Our AML Principal will ensure that all Supervising Principals and Operations staff receive sufficient training regarding our internal monitoring tools. The AML Principal will undertake a periodic review to assure that such tools are appropriately utilized and are sufficient for our specific monitoring needs. The AML Principal will also maintain records indicating review findings and that appropriate corrective measures are taken where required.

Our AML Principal will retain documentation of when and how our monitoring efforts are carried out, and will report suspicious activities to the appropriate authorities.

Information used to determine whether to file a SAR-SF will come from exception reports and includes, but is not necessarily limited to, transaction size, location, type, number and nature of the activity.

Our AML Principal may create employee guidelines that include examples of suspicious money laundering activity and lists of high-risk clients whose accounts may warrant further scrutiny. We will maintain copies of such guidelines in the files, indicating names of the individuals to whom the material was disseminated and dates of dissemination.

Our AML Principal will conduct appropriate investigations, in concert with all involved individuals and, if necessary with other members of Senior Management, before a SAR-SF is filed, and document all matters surrounding such investigation.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Monitoring Employee Conduct and Accounts

Designated Supervising Principal

Designated Supervisors will monitor employee conduct and employee accounts to ensure that individuals are not engaged in any money laundering activities. Designated Supervisors will work in concert with our AML Principal.

Supervisory Review Procedures and Documentation

Designated Supervisors and Compliance Surveillance will subject employee accounts to the same AML procedures as customer accounts.

Senior Management will review the actions taken by Managing Principals/Compliance Surveillance with the CCO and these results will be utilized to determine whether additional training or other corrective measures are necessary to improve our AML oversight. As part of our AML books and records we will also maintain documentation regarding any action taken as a result of the review.

If our AML Principal services accounts and acts as a designated supervising principal for any registered representatives, his or her personal accounts and performance will be reviewed by another member of Senior Management, whose name and title will be reflected on the documentation of all such reviews.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Monitoring for New Rules and New Procedures

Designated Supervising Principal

Our AML Principal will appropriately monitor the USA PATRIOT Act, Treasury and Bank Secrecy Act rules and regulations and guidance issued by FINRA, to be able to timely put into effect any new procedures governing either a specific type of account (i.e., Foreign Bank, Private Banking Account, Foreign Senior Official), specific transactions within an account (i.e., wire orders, large transactions, etc.), new or amended reporting requirements or new account monitoring requirements.

Supervisory Review Procedures and Documentation

Our AML Principal, or designee, will periodically review applicable websites, which may include the following websites, to determine whether new anti-money laundering procedures need to be put into effect.
www.finra.org

www.bankersonline.com

http://www.ustreas.gov/

http://www.fincen.gov/

http://www.fincen.gov/reg_bsaforms.html

Our AML Principal, or designee, may maintain documentation of periodic reviews, indicating what steps were taken, if necessary, to adjust our policies and procedures.

ANTI-MONEY LAUNDERING (AML) PROGRAM: National Security Letters (NSLs)

Designated Supervising Principal

Our AML Principal is responsible for appropriate handing of all National Security Letters received from our local Federal Bureau of Investigation or other federal government authority conducting counterintelligence and counterterrorism investigations to obtain, among other things, financial records.

Supervisory Review Procedures and Documentation

Our AML principal will ensure that AML training stresses the requirement that all NSL information remain 100% confidential. In addition, our AML principal will limit the dissemination of any NSLs received on a strict "need to know" basis in order to limit the possibilities that the confidentiality requirement be jeopardized. Any individuals found to have treated NSLs in a less-than-fully-confidential nature will be terminated and a determination will be made as to whether or not such a breach of policy will require the filing of a SAR.

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

ANTI-MONEY LAUNDERING (AML) PROGRAM: Notification of Suspicious Activity Report (SAR) Filings

Designated Supervising Principal

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

Supervisory Review Procedures and Documentation

All associated personnel are advised through AML training measures NOT to notify any person involved in the transaction that said transaction has been reported, except as permitted by Bank Secrecy Act (BSA)

regulations.

Our training includes instructions that 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.

We will also maintain documentation of all training related to this matter, indicating dates of such training and names and CRD #s of those who received the training.

**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."*

Regulatory Reference

FINRA Regulatory Notice 12-08 SEC January 26, 2012 letter

ANTI-MONEY LAUNDERING (AML) PROGRAM: Private Banking Accounts/Senior Foreign Political Figures

Background

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 or 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.

Designated Supervising Principal

Our AML Principal will ensure that all registered personnel appropriately handle private banking accounts and accounts for senior foreign political figures, including undertaking all required enhanced due diligence steps.

Each individual's immediate supervising principal is also responsible for ongoing oversight to ensure these situations are handled according to the rules and regulations as well as our internal policies and procedures.

Regardless of whether we have such accounts, we maintain these policies and procedures so we are prepared to immediately deal with the situation should it arise.

Supervisory Review Procedures and Documentation

Our AML Principal manages or oversees a due diligence program for all private banking accounts for non-U.S. persons that is designed to reasonably detect and report any known or suspected money laundering conducted through, or involving, any private banking account maintained by, or on behalf of, a non-U.S. person regardless of when such an account was opened.

Our AML Principal also ensures that accounts requested or maintained by, or on behalf of, senior foreign political figures, including their family members and close associates, receive enhanced due diligence scrutiny (Section 312, USA PATRIOT Act).

Minimally, the decision to open or maintain a private banking account or an account held by a senior foreign political figure must be approved by either our AML Principal or a member of Senior Management, with written approval indicated by initials and dates.

For private banking accounts or accounts determined to be held by a senior foreign political figure, the following due diligence procedures must occur prior to opening the account

- Ascertain the identity of all nominal holders and holders of any beneficial ownership interest in the account, including information on those holders' lines of business and sources of wealth
- Ascertain the source of funds deposited into the account
- Ascertain whether any such holder may be a senior foreign political figure
- Review the activity of the account to ensure it is consistent with information obtained about the source of the funds and with the states purpose and expected use of the account
- Report, in accordance with applicable law and regulation, any known or suspected violation of law conducted through or involving the account

We review public information, including information available in Internet databases, to determine whether any private banking account holders are senior foreign political figures. If we do not find any such information and the account holder states that he or she is not a senior foreign political figure, additional enhanced due diligence is not required. We will maintain documentation in our AML files that evidence the steps taken and rationale utilized to determine that no further due diligence was required.

However, if we discover information indicating that a particular private banking account holder may be a senior foreign political figure, and after taking additional reasonable steps to confirm this information, we determine that the individual is, in fact, a senior foreign political figure, we will conduct enhanced due diligence to detect and report transactions that may involve the proceeds of foreign corruption.

Such due diligence will consider the risk that the account funds may be the proceeds of foreign corruption. Our investigation will determine the purpose and use of the private banking account, the location of the account holders, source of account funds, the types of transactions engaged in through the account, and jurisdictions involved in such transactions. The degree of scrutiny applied will depend on various risk factors, including, but not limited to, whether the jurisdiction in which the senior foreign political figure is located is one in which current or former political figures have been implicated in corruption and the length of time that a political figure was in office.

Depending on the risk factors determined by discussions between the registered representative, supervising principal and our AML Principal, our enhanced due diligence may include

- Probing the account holder's employment history
- Scrutinizing the account holder's sources of funds
- Monitoring transactions to the extent necessary to detect and report proceeds of foreign corruption
- Reviewing monies coming from government, government-controlled or government-enterprise accounts (beyond salary amounts)

If due diligence cannot be performed adequately, further discussion between all relevant employees will be undertaken and our AML Principal will make a final determination whether to undertake one or more of the following actions

- Not open the account
- Suspend certain transactional activity
- File a SAR

- Close the account

Our AML Principal will ensure that appropriate documentation and notes are retained in the files regarding all discussions, and the rationale for the final decision.

In addition, for any private banking accounts we maintain, our AML Principal will ensure that the following are put into place and adhered to

- Written policies and procedures indicating exactly how to conduct enhanced due diligence efforts
- Company-wide notification of who is responsible for undertaking these efforts
- Designation of a specifically-named individual responsible for any reporting or additional requirements ensuing from the enhanced due diligence activities
- Procedures guaranteeing termination of correspondent relationships with a foreign bank no later than 10 business days after notification of such requirement by either the Secretary of the Treasury or the U.S. Attorney General

Our AML Principal will maintain documentation concerning all of the above and any other AML policies or procedures put into effect.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Recordkeeping

Designated Supervising Principal

Our AML Principal will ensure that all accounts are appropriately monitored to detect suspicious activity. In addition, each individual's immediate supervising principal is responsible for ongoing oversight to ensure that appropriate AML documents are retained in customer account files, as required.

Supervisory Review Procedures and Documentation

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 Private Client Services, LLC's 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. Any records stored off-site will be located to permit us complete access to all documents within a 24-hour period. 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 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, CTR, CMIR and FBAR filings
- 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

Regulatory Reference

Exchange Act Rule 17a-8

ANTI-MONEY LAUNDERING (AML) PROGRAM: Red Flags

Designated Supervising Principal

Our AML Principal will ensure that all registered personnel receive 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
- The customer engages in "Wash Sale" activity, or manipulative trading activity (i.e., Marking the Close, Pre- Block manipulation, and Pre-Arranged trades.)

Our AML training, conducted under the oversight of our AML Principal, 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.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Reliance on Another Financial Institution

Designated Supervising Principal

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.

Supervisory Review Procedures and Documentation

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 institutional 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)
- A copy of a contract between this broker-dealer 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 the USA PATRIOT Act are met, we remain solely responsible for applying our CIP Program to each customer in accordance with Section 326.

Regulatory Reference

FINRA Rule 3310
Section 326 of the USA PATRIOT Act

ANTI-MONEY LAUNDERING (AML) PROGRAM: Senior Management Approval of AML Program

Designated Supervising Principal

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.

Supervisory Review Procedures and Documentation

Minimally on an annual basis, the designated principal will review our AML Program and any reports resulting from testing of the Program, or correspondence prepared by our AML Principal concerning the Program, and any other relevant materials speaking to the strengths and weaknesses of the Program.

All materials reviewed for this purpose will be maintained in the AML files, such review being evidenced by initials and dates. If everything is found to be acceptable under the current program, the designated principal will be responsible for obtaining senior management approval and having the signed and dated document maintained in the AML files.

If the review determined that there needs to be some adjustments made to our AML Program, senior management and Compliance will meet with our AML Principal to determine what corrective measures need

to be taken before the "Senior Manager 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, timeframes for putting such corrective measures into effect, the names of the individuals responsible for ensuring corrective measures are followed up on, etc.

Regulatory Reference

FINRA Rule 3310
Section 352 of the USA PATRIOT Act

ANTI-MONEY LAUNDERING (AML) PROGRAM: Sharing Information with Other Financial Institutions

Designated Supervising Principal

Our AML Principal is responsible for ensuring that all AML-related information shared with other financial institutions is done in a manner that is compliant with the rules and regulations under the USA PATRIOT Act and FINRA Rule 3310.

Supervisory Review Procedures and Documentation

As deemed appropriate by our AML Principal and other members of Senior Management, we will share information about those suspected of terrorist financing and money laundering with other financial institutions for the purposes of identifying and reporting such suspicions and to determine whether to establish or maintain an account or engage in a transaction on behalf of the account.

Prior to sharing any such information, 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. 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.

We will use the notice form found at http://www.fincen.gov/fi_infoappb.html.

As the initial notice is good for only one year, our AML Principal will review all notices at least annually to ensure that, if we continue to share information with any given entity, another notice is filed both by us and the other entity. We will retain copies of all such continuation notice filings in our AML files.

Another manner in which we may 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. The quarterly list of USA PATRIOT Act Section 314(b) participants is available at http://www.fincen.gov/314bnoti.pdf. If we verify using this method, our AML Principal will know the password (which changes with each quarterly list). We will maintain copies of all such verifications in our AML files, evidencing the review with initials and dates.

Our AML Principal must ensure that strict procedures are in place so that only relevant information is shared and the security and confidentiality of this information is protected, including segregating it from the firm's other books and records.

Quarterly, our files will be reviewed to ensure that all such information has been successfully removed from client files and is 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 applicable.

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

In addition to sharing information with other financial institutions about possible terrorist financing and money laundering, we will also share information about particular suspicious transactions with our clearing broker to determine whether it is more appropriate for one of us to file a Suspicious Activity Report (SAR), or whether it is appropriate that both institutions file a SAR. Our AML Principal will maintain documentation of these discussions.

In any instance in which we file a SAR for a transaction handled by both this firm and another financial institution, it is permissible and often appropriate for us to 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 Principal will maintain documentation regarding all shared SAR filings as part of our AML books and records.

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.

As with all other books and records relating to our AML Program, our AML Principal will ensure that all records relating to sharing of information are retained for a five-year period.

Regulatory Reference

FINRA Rule 3310

ANTI-MONEY LAUNDERING (AML) PROGRAM: Suspicious Activity Report (SAR) Filing Deadlines

Designated Supervising Principal

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

Supervisory Review Procedures and Documentation

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 (required as of March 31, 2013), our AML Principal must ensure that we have registered with FinCEN by logging onto http://bsaefiling.fincen.treas.gov.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Testing/Auditing Program

Designated Supervising Principal

Our AML Principal will ensure that we conduct appropriate testing and auditing of our AML program in a timely manner.

Supervisory Review Procedures and Documentation

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.

We will maintain documentation of the decision that was made and the rationale for it, including if appropriate, the name of the outside party.

Our use of either internal or external parties to comply with this annual requirement will be reviewed to determine if any changes should be made. We will maintain dated and initialed documentation in the file indicating what changes, if any, need to be made, indicating the time frame for such changes.

FINRA Rule 3310 indicates that some limited broker-dealers may have their AML testing done on a two-year cycle. Our AML Principal will review Notice to Members 06-07, and if they determine that we can adopt the two- year testing cycle, the rationale for this determination will be maintained in the files. If we are on a two-year cycle, our AMP Principal will review the rationale annually to determine whether we can continue on this cycle or, due to a change in activities, we must change to a one-year review cycle.

Our AML Principal will ensure that appropriate annual AML program testing and auditing is undertaken, and that the findings are reported to Senior Management or to an internal audit committee. The AML Principal must also maintain appropriate documentation evidencing such submission 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. We will maintain documentation concerning all recommendations accepted (indicating time frames for implementing changes, indication of responsibilities, etc.), and the rationale for any decisions not to implement a recommendation, including documentation about why the change was considered not necessary, who made the decision, etc.

Regulatory Reference

FINRA Rule 3310

ANTI-MONEY LAUNDERING (AML) PROGRAM: The Travel Rule under the Bank Secrecy Act (BSA)

Background

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.

Designated Supervising Principal

Our AML Principal will ensure our compliance with all requirements under the BSA's travel rule and maintain documentation of all such efforts.

Supervisory Review Procedures and Documentation

We must maintain and keep certain specified information about the transmitter and recipient of transmitted funds of three thousand dollars ($3,000) or more, sent or received by us, including wire or electronic transfers. Additionally, we must include this information on the actual transmittal orders. Before such transfer can be made, a designated supervising principal must date and initial the transfer, indicating that we have obtained and disclosed the appropriate information.

Whenever a client requests that money be wired from his/her account, we, as the financial institution acting on behalf of the transmitter (i.e., the client), must include and send the following information in the wire transmittal order:

- The name of the transmitter
- 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

We may not wire any monies out of an account without the electronic approval or initialed and dated approval of a designated supervisory principal, indicating that all required information has been received and disclosed with the transmittal order.

When a client wires money into an account, we must obtain the following:

- The name of the recipient
- The address of the recipient
- The account number of the recipient
- Any other specific identifier of the recipient

A request to wire money to an account will be not approved without the electronic approval or initialed and dated approval of a designated supervising principal, indicating that all information has been obtained prior to acceptance of the wire transmittal.

To verify the identity of transmitters and recipients who are not established customers of the firm (i.e., customers of the firm who have not previously maintained an account with us or for whom we have not obtained and maintained a file with the customer's name, address, taxpayer identification number, or, if none, an alien identification number or passport number and country of issuance), such information will be obtained and maintained in the file. In such instances, the wire transfer request for funds out of an account or for funds into an account will not be approved until a designated supervising principal has indicated, by initialing and dating the request that all the required information has been obtained to the satisfaction of our Customer Identification Program (CIP) requirements. We will maintain this customer information in the file.

We will periodically review all wire transfers (in and out) to ensure that all appropriate information has been obtained and disclosed as required. We will maintain documentation of all such reviews, evidenced by dates, names of individuals conducting such reviews, copies of exception reports utilized to determine such activities, findings and any corrective measures taken.

ANTI-MONEY LAUNDERING (AML) PROGRAM: Training Programs

Designated Supervising Principal

Our AML Principal will ensure that all affiliated personnel, registered as well as those non-registered individuals requiring such training, receive 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.

Supervisory Review Procedures and Documentation

Our AML Principal will ensure that we maintain an ongoing 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.

Our AML Principal, working with Senior Management and Compliance, will determine whether such training will be developed and delivered internally or whether we will contract with a third-party for training assistance.

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 will include 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.

- Within a month of being hired, all registered and non-registered personnel deemed by nature of their specific job responsibilities to require such training may be required to undergo individual or group training overseen by our AML Principal
- 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.

Regulatory Reference

FINRA Rule 3310