Kingswood Capital, LLC
Anti-Money Laundering (AML)Program

Firm Policy

It is the policy of the firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the Bank Secrecy Act (BSA) and its implementing regulations.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have been derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Our AML policies, procedures and internal controls are designed to ensure compliance with all applicable BSA regulations and FINRA rules and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

AML Compliance Person Designation and Duties

The firm has designated Tyler Bashaw as its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the firm's AML program. Mr. Bashaw has a working knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge and training, including six years of compliance and surveillance monitoring experience.

The duties of the AML Compliance Person will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees, and updating procedures as required. The AML Compliance Person will also ensure that the firm keeps and maintains all of the required AML records and will ensure that Suspicious Activity Reports (SARs) are filed with the Financial Crimes Enforcement Network (FinCEN) when appropriate. The AML Compliance Person is vested with full responsibility and authority to enforce the firm's AML program.

The firm will provide FINRA with contact information for the AML Compliance Person, including: (1) name; (2) title; (3) mailing address; (4) email address; (5) telephone number; and (6) facsimile number through the FINRA Contact System (FCS). The firm will promptly notify FINRA of any change in this information through FCS and will review, and if necessary, update, this information within 17 business days after the end of each calendar year.

The annual review of FCS information will be conducted by the AMLCO or designee, and will be completed with all necessary updates being provided no later than 17 business days following the end of each calendar year. In addition, if there is any change to the information, the Firm will update the information promptly, but in any event not later than 30 days following the change.

FinCEN Requests Under USA PATRIOT Act Section 314(a)

We will respond to a Financial Crimes Enforcement Network (FinCEN) request concerning accounts and transactions (a 314(a) Request) by immediately searching our records to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity or organization named in the 314(a) Request as outlined in the Frequently Asked Questions (FAQ) located on FinCEN's secure Web site.

We understand that we have 14 days (unless otherwise specified by FinCEN) from the transmission date of the request to respond to a 314(a) Request. We will designate, through the FINRA Contact System (FCS) one or more persons to be the point of contact (POC) for 314(a) Requests and will promptly update the POC information following any change in such information. (*See also* Section 2 above regarding updating of contact information for the AML Compliance Person.) Unless otherwise stated in the 314(a) Request or specified by FinCEN, we will search those documents outlined in FinCEN's FAQ.

If we find a match, the Firm will report it to FinCEN via FinCEN's Web-based 314(a) Secure Information Sharing System within 14 days or within the time requested by FinCEN in the request. If the search parameters differ from those mentioned above (for example, if FinCEN limits the search to a geographic location), the Firm will structure our search accordingly.

We will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. The Firm will review, maintain and implement procedures to protect the security and confidentiality of requests from FinCEN similar to those procedures established to satisfy the requirements of Section 501 of the Gramm- Leach-Bliley Act with regard to the protection of customers' nonpublic information. We will direct any questions we have about the 314(a) Request to the requesting federal law enforcement agency as designated in the request. Unless otherwise stated in the 314(a) Request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the periodic 314(a) Requests as a government provided list of suspected terrorists for purposes of the customer identification and verification requirements.

National Security Letters

National Security Letters (NSLs) are written investigative demands that may be issued by the local Federal Bureau of Investigation and other federal government authorities conducting counterintelligence and counterterrorism investigations to obtain, among other things, financial records of broker-dealers. NSLs are highly confidential. No broker-dealer, officer, employee or agent of the broker-dealer can disclose to any person that a government authority or the FBI has sought or obtained access to records. Firms that receive NSLs must have policies and procedures in place for processing and maintaining the confidentiality of NSLs**.** In the event a Suspicious Activity Report (SAR) is filed after receiving a NSL, the SAR will not contain any reference to the receipt or existence of the NSL.

Grand Jury Subpoenas

We understand that the receipt of a grand jury subpoena concerning a customer does not in itself require that we file a Suspicious Activity Report (SAR). When we receive a grand jury subpoena, we will conduct a risk assessment of the customer subject to the subpoena as well as review the customer's account activity. If we uncover suspicious activity during our risk assessment and review, we will elevate that customer's risk assessment and file a SAR in accordance with the SAR filing requirements. We understand that none of our officers, employees or agents may directly or indirectly disclose to the person who is the subject of the subpoena its existence, its contents or the information we used to respond to it. To maintain the confidentiality of any grand jury subpoena we receive, we will process and maintain the subpoena by senior compliance handling in accordance with required event. If we file a SAR after receiving a grand jury subpoena, the SAR will not contain any reference to the receipt or existence of the subpoena. The SAR will only contain detailed information about the facts and circumstances of the detected suspicious activity.

Voluntary Information Sharing With Other Financial Institutions Under USA PATRIOT Act Section 314(b)

We will share information with other financial institutions regarding individuals, entities, organizations and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering. The AMLCO will ensure that the firm files with FinCEN an initial notice before any sharing occurs and annual notices thereafter. We will use the notice form found at FinCEN's Web site. Before we share information with another financial institution, we will take reasonable steps to verify that the other financial institution has submitted the requisite notice to FinCEN, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that FinCEN will make available. We understand that this requirement applies even to financial institutions *with which we are affiliated*, and that we will obtain the requisite notices from affiliates and follow all required procedures.

We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, for example, by segregating it from the firm's other books and records.We also will employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:

1. identifying and, where appropriate, reporting on money laundering or terrorist activities.
2. determining whether to establish or maintain an account, or to engage in a transaction; or
3. assisting the financial institution in complying with performing such activities.

Joint Filing of SARs by Broker-Dealers and Other Financial Institutions

We will file joint SARs in the following circumstances, according to the nature of the activity. We will also share information about a particular suspicious transaction with any broker dealer, as appropriate, involved in that particular transaction for purposes of determining whether we will file jointly a SAR. We will share information about particular suspicious transactions with our clearing broker for purposes of determining whether we and our clearing broker will file jointly a SAR. In cases in which we file a joint SAR for a transaction that has been handled both by us and by the clearing broker, we may share with the clearing broker a copy of the filed SAR.

If we determine it is appropriate to jointly file a SAR, we understand that we cannot disclose that we have filed a SAR with any financial institution except the financial institution that is filing jointly. If we determine it is not appropriate to file jointly (*e.g.*, because the SAR concerns the other broker-dealer or one of its employees), we understand that we cannot disclose that we have filed a SAR to any other financial institution or insurance company.

Checking the Office of Foreign Assets Control Listings

Before opening an account, and on an ongoing basis, the Firm will check to ensure that each new customer does not appear on the SDN list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC. (*See* the OFAC Web site for the SDN list and listings of current sanctions and embargoes). Because the SDN list and listings of economic sanctions and embargoes are updated frequently, we will consult them on a regular basis and subscribe to receive any available updates when they occur.

With respect to the SDN list, we may also access that list through various software programs to ensure speed and accuracy. *See also* FINRA's OFAC Search Tool that screens names against the SDN list. The Firm will also review existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated and be tracked through the RBC back-office system. Such SDN / OFAC list review is documented with the new account paperwork. Each search is printed and imaged with the new account paperwork and maintained in the client file. Further, our clearing firms, RBC, Raymond James APEX, notify our Firm by email alert if a potential match is found after an account is opened with RBC. The FinCEN SISS list is used for scrubbing electronically for existing clients as the list is updated.

If we determine that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC, we will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC within 10 days. We will also call the OFAC Hotline at (800) 540-6322 immediately.

Our review will include customer accounts, transactions involving customers (including activity that passes through the firm such as wires) and the review of customer transactions that involve physical security certificates or application-based investments (*e.g.*, mutual funds).

The Firm will randomly test their systems to ensure that the OFAC checking system is performing as expected and required, including a check for name mis- spellings or derivations of blocked persons to be sure that they will be flagged when screened through OFAC. All results will be documented for the file. These "soft hits" or potential matches are tracked, reviewed, and results of the review are documented.

Customer Identification Program

In addition to the information we must collect under FINRA Rule 2010 (Standards of Commercial Honor and Principles of Trade), NASD Rules 2310 (Recommendations to Customers - Suitability) and 3110 (Books and Records) and Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3(a)(9) (Beneficial Ownership regarding Cash and Margin Accounts) and 17a-3(a)(17) (Customer Accounts), we have established, documented and maintained a written Customer Identification Program (CIP).

We will collect certain minimum customer identification information from each customer who opens an account; utilize risk-based measures to verify the identity of each customer who opens an account; record customer identification information and the verification methods and results; provide the required adequate CIP notice to customers that we will seek identification information to verify their identities; and compare customer identification information with government-provided lists of suspected terrorists, once such lists have been issued by the government. *See* Section 5.g. (Notice to Customers) for additional information.

Required Customer Information

Prior to opening an account, the Firm will collect the following information for all accounts, if applicable, for any person, entity or organization that is opening a new account and whose name is on the account:

1. the name;
2. date of birth (for an individual);
3. an address, which will be a residential or business street address (for an individual), an Army Post Office (APO) or Fleet Post Office (FPO) box number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address), or a principal place of business, local office, or other physical location (for a person other than an individual); and
4. an identification number, which will be a taxpayer identification number (for U.S. persons), or one or more of the following: a taxpayer identification number, passport number and country of issuance, alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard (for non-U.S. persons).

For greater clarity for requirements by specific account type, the firm has created the following table.

Account type, and documentation/information required:	**Minimum information to collect, review and verify prior to or at account opening. If Firm does not accept any of the following types of accounts, it is so stated here:**
For individual accounts	1 Net worth 1 Annual income 1 Occupation and employment data 1 Investment experience and objectives 1 Copy of valid driver's license, passport or other valid government issued form of identification with photo
For individual, non-US person accounts	Passport or alien identification card number OR 1 Number and country of issuance of other government-issued documents bearing a photograph or other safeguard
Domestic operating or commercial entities	Collect copies of documents such as certificate of incorporation, business license, partnership agreements, and corporate resolutions. Additionally, 1 Information used to determine business's identity 1 The authority of its rep. to act on its behalf.

Domestic trusts	Collect samples of trust formation and authorization docs. Identify: 1 Name of trustee 1 Activity authorized by trust 1 The authority of trust's rep. to act on its behalf.
Foreign and offshore entities	1 Identity of account holder and other persons or entities authorized to trade for the account 1 Country of incorporation 1 Location of entity **We generally do not open these types of accounts. Any attempt to open this type of account should be reported to our AMLCO immediately.**
Institutional accounts, hedge funds, investment funds and other intermediary relationships	Maintain examples of efforts to explore and document these considerations in client file. Evaluate the following, where applicable: ◆ 1. 1 The institution or intermediary has authority to act on behalf of the underlying client (written representation of this authority) 1 The institutional client/intermediary has policies and procedures to know its clients 1 The institution/intermediary has established anti-money laundering policies and procedures ◆ 2. 1 The Firm has historical experience with the institution/intermediary 3.

	1 The institution/intermediary is a registered financial institution based in a major regulated financial center or is a registered financial institution located in an FATF jurisdiction 1 The institution/intermediary has a reputable history in the investment business 1 The institution/intermediary is from a jurisdiction characterized as an offshore banking or secrecy haven or is designated as a non-cooperative country by credible international organizations or multilateral expert groups
Accounts in high risk and non-cooperative jurisdictions Check lists in order to make informed decision: FATF, FinCEN, and U.S. Dept. of State's annual International Narcotics Control Strategy Report ("INCSR").	**We do not open these types of accounts, without exception. Any attempt to open this type of account should be reported to the AMLCO immediately.**
Accounts of senior foreign government or public officials (or their family members or close associates)	**We do not open these types of accounts, without exception. Any attempt to open this type of account should be reported to AMLCO immediately.**
Private Banking Accounts	1 Must verify the identity of all owners (nominal and beneficial) in the account, and information on these owners' lines of business and source of wealth 1 The source of funds deposited into the account 1 Whether such owners are senior foreign political figures (see above) NOTE: This applies to all such accounts, not just new accounts.

Foreign Correspondent Accounts and Foreign Shell Banks Rep should determine if correspondent account is for foreign shell bank or used to provide services to foreign shell bank; close account, if so, if account already exists, and contact AMLCCO. The Firm does not allow Foreign Correspondent Accounts or Foreign	**We do not open these types of accounts, without exception. Any attempt to open this type of account should be reported to AMLCO immediately.**
Shell Bank Accounts. NOTE: This applies to all such accounts, not just new accounts.	

In the event that a customer has applied for, but has not received, a taxpayer identification number, we will gather any pertinent information evidencing application for taxpayer identification number, residency and legal ability to invest to confirm that the application was filed before the customer opens the account and to obtain the taxpayer identification number within a reasonable period of time after the account is opened.

When opening an account for a foreign business or enterprise that does not have an identification number, we will request alternative government-issued documentation certifying the existence of the business or enterprise.

Customers Who Refuse to Provide Information

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

Verifying Information

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. The Firm will analyze the information we obtain to determine whether the information is sufficient to form a

reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

We will verify customer identity through documentary means, non-documentary means or both. We will use documents to verify customer identity when appropriate documents are available. Considering the industry's reported increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary.

We may also use non-documentary means, if we are still uncertain about whether we know the true identity of the customer. In verifying the information, we will consider whether the identifying information that we receive, such as the customer's name, street address, zip code, telephone number (if provided), date of birth and Social Security number, allow us to determine that we have a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

Appropriate documents for verifying the identity of customers include the following:

For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and

For a person, other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument.

We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity. We will also ensure the form of identity used is not expired.

We will use the following non-documentary methods of verifying identity:

1. 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 such as an identify reporting agency or database.
2. Checking references with other financial institutions; or
3. Obtaining a financial statement.

We will use non-documentary methods of verification when:

1. The customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard.

2. The firm is unfamiliar with the documents the customer presents for identification verification.
3. The customer and firm do not have face-to-face contact; and
4. There are other circumstances that increase the risk that the firm will be unable to verify the true identity of the customer through documentary means.

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

We recognize that the risk that we may not know the customer's true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated by the U.S. as a primary money laundering jurisdiction, a terrorist concern, or has been designated as a non-cooperative country or territory.

We will identify customers that pose a heightened risk of not being properly identified. We will also take the following additional measures that may be used to obtain information about the identity of the individuals associated with the customer when standard documentary methods prove to be insufficient: our operations department will gather any and all information necessary to determine eligibility and legality of individual or entity seeking to open an account through any and all methods available to us.

Lack of Verification

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (1) not open an account; (2) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity; (3) close an account after attempts to verify customer's identity fail; and (4) determine whether it is necessary to file a SAR in accordance with applicable laws and regulations.

Recordkeeping

We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. We will also keep records containing a

description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We will retain records of all identification information for five years after the account has been closed; we will retain records made about verification of the customer's identity for five years after the record is made.

Comparison with Government-Provided Lists of Terrorists

At such time as we receive notice that a federal government agency has issued a list of known or suspected terrorists and identified the list as a list for CIP purposes, we will, within a reasonable period of time after an account is opened (or earlier, if required by another federal law or regulation or federal directive issued in connection with an applicable list), determine whether a customer appears on any such list of known or suspected terrorists or terrorist organizations issued by any federal government agency and designated as such by Treasury in consultation with the federal functional regulators. We will follow all federal directives issued in connection with such lists.

We will continue to comply separately with OFAC rules prohibiting transactions with certain foreign countries or their nationals.

Notice to Customers

We will provide notice to customers that the firm is requesting information from them to verify their identities, as required by federal law. We will use the following method to provide notice to customers: through verbal disclosure at the time of account opening and written disclosure.

Reliance on Another Financial Institution for Identity Verification

We may, under the following circumstances, rely on the performance by another financial institution (including an affiliate) of some or all of the elements of our CIP with respect to any customer that is opening an account or has established an account or similar business relationship with the other financial institution to provide or engage in services, dealings or other financial transactions:

1. when such reliance is reasonable under the circumstances.

2. when the other financial institution is subject to a rule implementing the anti- money laundering compliance program requirements of 31 U.S.C. § 5318(h), and is regulated by a federal functional regulator; and

3. when the other financial institution has entered into a contract with our firm requiring it to certify annually to us that it has implemented its anti-money laundering program and that it will perform (or its agent will perform) specified requirements of the customer identification program.

We are aware that the ultimate responsibility of identity verification for Kingswood Capital, LLC customers, rests with the Firm, regardless of any contractual agreement with another financial institution to provide this verification service. The CCO is responsible for ensuring any contracted vendor or other financial institution engaged is conducting adequate verification, as and when appropriate, when the Firm will rely on that particular service.

Validating Customer Address Changes

The Firm will verify that in the event we receive a request for a change of address from an existing customer; certain procedures are followed as an effective verification process for requested address changes.

The designated supervisor will ensure that a notification letter is sent to the last known residential address of record for the customer as provided on the Firm's customer account information. Similar to a "negative verification" letter, this letter will confirm the requested address change which would require a response from the customer **only** in the event that the information contained in the confirmation letter is incorrect. Additionally, a similar verification letter will be sent to the new and/or current residential address also confirming the requested change. This is processed through the Firm's clearing firm, RBC.

The Operations Manager will verify a negative consent letter was sent through our clearing firms and will keep a copy in the client file. In the event a letter is not sent, we will send a separate negative consent letter. As an alternative method to verifying the change in customer address information, the Firm may contact the customer directly via telephone and receive verbal confirmation. All methods of the verification process shall be documented and retained as evidence of supervision and compliance in the customer file.

General Customer Due Diligence

It is important to our AML and SAR reporting program that we obtain sufficient information about each customer to allow us to evaluate the risk presented by that customer and to detect and report suspicious activity. When we open an account for a customer, the due diligence we perform may be in addition to customer information obtained for purposes of our CIP.

For each account meeting the following criteria: high net worth, recent increase in funds, corporate accounts, and non-United States citizens, we will take steps to obtain sufficient customer information to comply with our suspicious activity reporting requirements. Such information should include:

1. the customer's business;
2. the customer's anticipated account activity (both volume and type);
3. the source of the customer's funds.

For accounts that we have deemed to be higher risk, we will obtain the following information:

4. the purpose of the account;
5. the source of funds and wealth;
6. the beneficial owners of the accounts;
7. the customer's (or beneficial owner's) occupation or type of business;
8. financial statements;
9. banking references;
10. domicile (where the customer's business is organized);
11. description of customer's primary trade area and whether international transactions are expected to be routine;
12. description of the business operations and anticipated volume of trading;
13. explanation for any changes in account activity.

We will also ensure that the customer information remains accurate by sending out a three year mailing requesting account information updates, should any apply regarding current retained information.

Detecting and Closing Correspondent Accounts of Foreign Shell Banks

We do not open or maintain correspondent accounts for foreign shell banks. We will identify foreign shell bank accounts and any such account that is a correspondent account (any account that is established for a foreign shell bank to receive deposits from, or to make payments or other disbursements on behalf of, the foreign shell bank, or to handle other financial transactions related to such foreign shell bank) will immediately be closed and referred to the AMLCO. Upon finding or suspecting such accounts, firm employees will notify the AMLCO, who will terminate any verified correspondent account in the United States for a foreign shell bank. We will also terminate any correspondent account that we have determined is not maintained by a foreign shell bank but is being used to provide services to such a shell bank. We will exercise caution regarding liquidating positions in such accounts and take reasonable steps to ensure that no new positions are established in these accounts during the termination period. We will terminate any correspondent account for which we have not obtained the information described in Appendix A of the regulations regarding shell banks within the time periods specified in those regulations.

Certifications

We will require our foreign bank account holders to identify the owners of the foreign bank if it is not publicly traded, the name and street address of a person who resides in the United States and is authorized and has agreed to act as agent for acceptance of legal process, and an assurance that the foreign bank is not a shell bank nor is it facilitating activity of a shell bank. In lieu of this information the foreign bank may submit the Certification Regarding Correspondent Accounts For Foreign Banks provided in the BSA regulations. We will re-certify when we believe that the information is no longer accurate or at least once every three years.

Recordkeeping for Correspondent Accounts for Foreign Banks

We will 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.

Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationships with Foreign Bank

When we receive a written request from a federal law enforcement officer for information identifying the non-publicly traded owners of any foreign bank for which we maintain a correspondent account in the United States and/or the name and address of a person residing in the United States who is an agent to accept service of legal process for a foreign bank's correspondent account, we will provide that information to the requesting officer not later than seven days after receipt of the request. We will close, within 10 days, any correspondent account for a foreign bank that we learn from FinCEN, or the

Department of Justice has failed to comply with a summons or subpoena issued by the Secretary of the Treasury or the Attorney General of the United States or has failed to contest such a summons or subpoena. We will scrutinize any correspondent account activity during that 10-day period to ensure that any suspicious activity is appropriately reported and to ensure that no new positions are established in these correspondent accounts.

Due Diligence and Enhanced Due Diligence Requirements for Correspondent Accounts of Foreign Financial Institutions

Due Diligence for Correspondent Accounts of Foreign Financial Institutions

We do not open or maintain Correspondent Accounts of Foreign Financial Institutions. We will conduct an inquiry to determine whether a foreign financial institution has a correspondent account established, maintained, administered or managed by the firm and take immediate steps to close the account.

If we have correspondent accounts for foreign financial institutions, we will assess the money laundering risk posed, based on consideration of relevant risk factors. We can apply all, or a subset of these risk factors, depending on the nature of the foreign financial institutions and the relative money laundering risk posed by such institutions.

The relevant risk factors may include:

i. the nature of the foreign financial institution's business and the markets it serves;
ii. the type, purpose and anticipated activity of such correspondent account;
iii. the nature and duration of the firm's relationship with the foreign financial institution and its affiliates;
iv. the anti-money laundering and supervisory regime of the jurisdiction that issued the foreign financial institution's charter or license and, to the extent reasonably available, the jurisdiction in which any company that is an owner of the foreign financial institution is incorporated or chartered; and
v. information known or reasonably available to the covered financial institution about the foreign financial institution's anti-money laundering record.

In addition, our due diligence program will consider additional factors that have not been enumerated above when assessing foreign financial institutions that pose a higher risk of money laundering.

We will apply our risk-based due diligence procedures and controls to each foreign financial institution correspondent account on an ongoing basis. This includes periodically reviewing the activity of each foreign financial institution correspondent sufficient to ensure whether the nature and volume of account activity is generally consistent with the information regarding the purpose

and expected account activity and to ensure that the firm can adequately identify suspicious transactions. Ordinarily, we will not conduct this periodic review by scrutinizing every transaction taking place within the account. One procedure we may use instead is to use any account profiles for our correspondent accounts (to the extent we maintain these) that we ordinarily use to anticipate how the account might be used and the expected volume of activity to help establish baselines for detecting unusual activity.

Enhanced Due Diligence

We will assess any correspondent accounts for foreign financial institutions to determine whether they are correspondent accounts that have been established, maintained, administered or managed for any foreign bank that operates under:

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

If we determine that we have any correspondent accounts for these specified foreign banks, we will perform enhanced due diligence on these correspondent accounts. The enhanced due diligence that we will perform for each correspondent account will include, at a minimum, procedures to take reasonable steps to:

- conduct enhanced scrutiny of the correspondent account to guard against money laundering and to identify and report any suspicious transactions. Such scrutiny will not only reflect the risk assessment that is described in Section 8.a. above, but will also include procedures to, as appropriate:
- obtain (*e.g.,* using a questionnaire) and consider information related to the foreign bank's AML program to assess the extent to which the foreign bank's correspondent account may expose us to any risk of money laundering;
- monitor transactions to, from or through the correspondent account in a manner reasonably designed to detect money laundering and suspicious activity (this monitoring may be conducted manually or electronically and may be done on an individual account basis or by product activity); and
- obtain information from the foreign bank about the identity of any person with authority to direct transactions through any correspondent account that is a payable-through account (a correspondent account maintained for a foreign bank through which the foreign bank permits its customer to engage, either directly or through a subaccount, in banking

activities) and the sources and beneficial owners of funds or other assets in the payable-through account.

- determine whether the foreign bank maintains correspondent accounts for other foreign banks that enable those other foreign banks to gain access to the correspondent account under review and, if so, to take reasonable steps to obtain information to assess and mitigate the money laundering risks associated with such accounts, including, as appropriate, the identity of those other foreign banks; and
- if the foreign bank's shares are not publicly traded, determine the identity of each owner and the nature and extent of each owner's ownership interest. We understand that for purposes of determining a private foreign bank's ownership, an "owner" is any person who directly or indirectly owns, controls or has the power to vote 10 percent or more of any class of securities of a foreign bank. We also understand that members of the same family shall be considered to be one person.

Special Procedures When Due Diligence or Enhanced Due Diligence Cannot Be Performed

In the event there are circumstances in which we cannot perform appropriate due diligence with respect to a correspondent account, we will refuse to open the account, and suspend transaction activity, file a SAR, close the correspondent account and/or take other appropriate action.

Kingswood Capital, LLC's policy is to NOT open foreign accounts. Any exception would only be with the prior review and written approval by the AMLCO.

Due Diligence and Enhanced Due Diligence Requirements for Private Banking Accounts/Senior Foreign Political Figures

We do not open or maintain private banking accounts.

Compliance with FinCEN's Issuance of Special Measures Against Foreign Jurisdictions, Financial Institutions or International Transactions of Primary Money Laundering Concern

We do not maintain any accounts (including correspondent accounts) with any foreign jurisdiction or financial institution. However, if FinCEN issues a final rule imposing a special measure against one or more foreign jurisdictions or financial institutions, classes of international transactions or types of accounts deeming them to be of primary money laundering concern, we understand that we must read FinCEN's final rule and follow any prescriptions or prohibitions contained in that rule.

Monitoring Accounts for Suspicious Activity

The Firm will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business. (Red flags are identified in Section 11.b. below.) Monitoring will be conducted through manual and automated methods.

- automated monitoring, generally for brokerage account activities through RBC, we will use RBC exception reports, daily transaction reports, money-line cash activity reports, wire transfer activity reports and third-party payments reports.
- manual monitoring, generally for non-brokerage account activities such as direct purchases in mutual funds, variable and fixed annuities, limited partnerships, private placements of securities and some REIT purchases.

The AMLCO or her designee (which may include the account representative's designated supervising principal) will be responsible for this monitoring, will review any activity that our monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

The Firm will conduct reviews of activity that our monitoring system detects and we will document our monitoring and reviews either electronically in the firm's system or written means and placed in the customer file. The AMLCO or her designee will conduct an appropriate investigation and review relevant information from internal or third- party sources before a SAR is filed.

1. Emergency Notification to Law Enforcement by Telephone

In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, we will immediately call an appropriate law enforcement authority. If a customer or company appears on OFAC's SDN list, we will call the OFAC Hotline at (800) 540-6322. Other contact numbers we will use are: FinCEN's Financial Institutions Hotline ((866) 556-3974) (especially to report transactions relating to terrorist activity), local U.S. Attorney's office (858) 268-5300, local FBI office (858) 565-1255 and local SEC office (323) 965-3998 (to voluntarily report such violations to the SEC in addition to contacting the appropriate law enforcement authority). If we notify the appropriate law enforcement authority of any such activity, we must still file a timely SAR.

Although we are not required to, in cases where we have filed a SAR that may require immediate attention by the SEC, we may contact the SEC via the SEC SAR Alert Message Line at (202) 551-SARS (7277) to alert the SEC about the filing. We understand that calling the SEC SAR Alert Message Line does not alleviate our obligations to file a SAR or notify an appropriate law enforcement authority.

2. Red Flags

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

Customers – Insufficient or Suspicious Information

- Provides unusual or suspicious identification documents that cannot be readily verified.
- Reluctant to provide complete information about nature and purpose of business, prior banking relationships, anticipated account activity, officers and directors or business location.
- Refuses to identify a legitimate source for funds or information is false, misleading or substantially incorrect.
    - Background is questionable or differs from expectations based on business activities.
    - Customer with no discernable reason for using the firm's service.

Efforts to Avoid Reporting and Recordkeeping

- Reluctant to provide information needed to file reports or fails to proceed with transaction.
- Attempts to persuade an employee not to file required reports or not to maintain required records.
- "Structures" deposits, withdrawals or purchase of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements.
- Unusual concern with the firm's compliance with government reporting requirements and firm's AML policies.

Certain Funds Transfer Activities

- Wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent business reason.
- Many small, incoming wire transfers or deposits made using checks and money orders. Almost immediately withdrawn or wired out in manner inconsistent with customer's business or history. May indicate a Ponzi scheme.
- Wire activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.

Certain Deposits or Dispositions of Physical Certificates

- Physical certificate is titled differently than the account.
- Physical certificate does not bear a restrictive legend, but based on history of the stock and/or volume of shares trading, it should have such a legend.
- Customer's explanation of how he or she acquired the certificate does not make sense or changes.
- Customer deposits the certificate with a request to journal the shares to multiple accounts, or to sell or otherwise transfer ownership of the shares.

Certain Securities Transactions

- Customer engages in prearranged or other non-competitive trading, including wash or cross trades of illiquid securities.
- Two or more accounts trade an illiquid stock suddenly and simultaneously.
- Customer journals securities between unrelated accounts for no apparent business reason.
- Customer has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason.
- Customer transactions include a pattern of receiving stock in physical form or the incoming transfer of shares, selling the position and wiring out proceeds.
- Customer's trading patterns suggest that he or she may have inside information.

Transactions Involving Penny Stock Companies

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

Transactions Involving Insurance Products

- Cancels an insurance contract and directs funds to a third party.
- Structures withdrawals of funds following deposits of insurance annuity checks signaling an effort to avoid BSA reporting requirements.
- Rapidly withdraws funds shortly after a deposit of a large insurance check when the purpose of the fund withdrawal cannot be determined.
- Cancels annuity products within the free look period which, although could be legitimate, may signal a method of laundering funds if accompanied with other suspicious indicia.
- Opens and closes accounts with one insurance company then reopens a new account shortly thereafter with the same insurance company, each time with new ownership information.
- Purchases an insurance product with no concern for investment objective or performance.
- Purchases an insurance product with unknown or unverifiable sources of funds, such as cash, official checks or sequentially numbered money orders.

Activity Inconsistent With Business

- Transactions patterns show a sudden change inconsistent with normal activities.
- Unusual transfers of funds or journal entries among accounts without any apparent business purpose.
- Maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
- Appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.

Other Suspicious Customer Activity

- Unexplained high level of account activity with very low levels of securities transactions.
- Funds deposits for purchase of a long-term investment followed shortly by a request to liquidate the position and transfer the proceeds out of the account.
- Law enforcement subpoenas.
- Large numbers of securities transactions across a number of jurisdictions.

- Buying and selling securities with no purpose or in unusual circumstances (*e.g.*, churning at customer's request).
- Payment by third-party check or money transfer without an apparent connection to the customer.
- Payments to third-party without apparent connection to customer.
- No concern regarding the cost of transactions or fees (*i.e.*, surrender fees, higher than necessary commissions, etc.).

Responding to Red Flags and Suspicious Activity

When an employee of the firm detects any red flag, or other activity that may be suspicious, he or she will notify the chief compliance officer. Under the direction of the AML Compliance Person, the firm will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or filing a SAR.

Suspicious Transactions and BSA Reporting

Filing a SAR

We will file SARs with FinCEN for any transactions (including deposits and transfers) conducted or attempted by, at or through our firm involving $5,000 or more of funds or assets (either individually or in the aggregate) where we know, suspect or have reason to suspect:

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

We will also file a SAR and notify the appropriate law enforcement authority in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes. In addition, although we are not required to, we may contact that SEC in cases where a SAR we have filed may require immediate attention by the SEC. *See* Section 11 for contact numbers. We also understand that, even if we notify a regulator of a violation, unless it is specifically covered by one of the exceptions in the SAR rule, we must file a SAR reporting the violation.

We may file a voluntary SAR for any suspicious transaction that we believe is relevant to the possible violation of any law or regulation but that is not required to be reported by us under the SAR rule. It is our policy that all SARs will be reported regularly to the Board of Directors and appropriate senior management, with a clear reminder of the need to maintain the confidentiality of the SAR.

We will report suspicious transactions by completing a SAR, and we will collect and maintain supporting documentation as required by the BSA regulations. We will file a SAR no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR. 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. The phrase "initial detection" does not mean the moment a transaction is highlighted for review. The 30-day (or 60-day) period begins when an appropriate review is conducted and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR requirements. A review must be initiated promptly upon identification of unusual activity that warrants investigation.

We will retain copies of any SAR filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR. We will identify and maintain supporting documentation and make such information available to FinCEN, any other appropriate law enforcement agencies, federal or state securities regulators or SROs upon request.

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the BSA regulations. We understand that anyone who is subpoenaed or required to disclose a SAR or the information contained in the SAR will, except where disclosure is requested by FinCEN, the SEC, or another appropriate law enforcement or regulatory agency, or an SRO registered with the SEC, decline to produce the SAR or to provide any information that would disclose that a SAR was prepared or filed. We will notify FinCEN of any such request and our response.

The Firm will **not** file a SAR, and specifically, will determine that it is **not** appropriate to file a SAR report, when there is the **absence** of knowing, suspecting or having reason to suspect:

- the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;

- the transaction is designed, whether through structuring or otherwise, 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;
- situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes. In addition, although we are not required to, we may contact that SEC in cases where a SAR we have filed may require immediate attention by the SEC. *See* Section 11 for contact numbers. We also understand that, even if we notify a regulator of a violation, unless it is specifically covered by one of the exceptions in the SAR rule, we must file a SAR reporting the violation; or
- any suspicious transaction that we believe is relevant to the possible violation of any law or regulation but that is not required to be reported by us under the SAR rule.

Currency Transaction Reports

Our firm prohibits transactions involving currency and has the following procedures to prevent such transactions: all account openings must be approved by our home office, Kingswood Capital's clearing firms will not hold foreign currency or precious metals. If we discover such transactions have occurred, we will file with FinCEN CTRs for currency transactions that exceed $10,000. Also, we will treat multiple transactions involving currency as a single transaction for purposes of determining whether to file a CTR if they total more than $10,000 and are made by or on behalf of the same person during any one business day. We will use the CTR Form provided on FinCEN's Web site.

Currency and Monetary Instrument Transportation Reports

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

purpose of evading the reporting requirements, on one or more days). We will use the CMIR Form provided on FinCEN's Web site.

Foreign Bank and Financial Accounts Reports

We will file a FBAR with the IRS for any financial accounts of more than $10,000 that we hold, or for which we have signature or other authority over, in a foreign country. We will use the FBAR Form provided on the IRS's Web site.

Monetary Instrument Handling

The Firm does not issue monetary instruments, including bank checks or drafts, cashier's checks, money orders or traveler's checks.

The receipt of monetary instruments is handled as follows:

- The Firm does not accept cashier's checks, traveler's checks, money orders, or promissory notes. Any of those instruments submitted to us for deposit are returned to the client on the same business day as receipt. If received by mail, they will be returned to the client on the same business day along with a letter of explanation and instructions for acceptable future payment. Evidence of rejection or return is documented in both the client's file and the Funds Received and Delivered log through our document imaging database with a copy of the letter.
- The Firm does not accept bank checks or third-party checks over the amount of $1000. If received by mail, they will be returned to the client on the same business day along with a letter of explanation and instructions for acceptable future payment. Evidence of rejection or return is documented in both the client's file and the Funds Received and Delivered log through our document imaging database with a copy of the letter. We do accept bank and third-party checks under 1000. These checks are identified as such in our document imaging database. Surveillance reports of these deposits are reviewed periodically by the AML Compliance Officer (AMLCO) to ensure compliance with AML regulations.

Funds Transmittals of $3,000 or More Under the Travel Rule

When we are the transmittor's financial institution in funds of $3,000 or more, we will retain either the original or a copy (*e.g.*, microfilm, electronic record) of the transmittal order. We will also record on the transmittal order the following information: (1) the name and address of the transmittor; (2) if the payment is ordered from an account, the account number; (3) the amount of the transmittal order; (4) the execution date of the transmittal order; and (5) the identity of the recipient's financial institution. In addition, we will include on the transmittal order as many of the following items of information as are received with the transmittal order: (1) the name and address of the recipient; (2) the account

number of the recipient; (3) any other specific identifier of the recipient; and (4) any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order.

We will also verify the identity of the person placing the transmittal order (if we are the transmitting firm), provided the transmittal order is placed in person and the transmittor is not an established customer of the firm (*i.e.*, a customer of the firm who has 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, alien identification number or passport number and country of issuance).

If a transmittor or recipient is conducting business in person, we will obtain: (1) the person's name and address; (2) the type of identification reviewed and the number of the identification document (*e.g.,* driver's license); and (3) the person's taxpayer identification number (*e.g.,* Social Security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record the lack thereof.

If a transmittor or recipient is not conducting business in person, we shall obtain the person's name, address, and a copy or record of the method of payment (*e.g.,* check or credit card transaction). In the case of transmittors only, we shall also obtain the transmittor's taxpayer identification number (*e.g.,* Social Security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof. In the case of recipients only, we shall obtain the name and address of the person to which the transmittal was sent.

AML Recordkeeping

Responsibility for Required AML Records and SAR Filing

Our AML Compliance Person and his or her designee will be responsible for ensuring that AML records are maintained properly, and that SARs are filed as required.

In addition, as part of our AML program, our firm will create and maintain SARs, CTRs, CMIRs, FBARs, and relevant documentation on customer identity and verification *(See* Section 5 above) and funds transmittals. We will maintain SARs and their accompanying documentation for at least five years.

We will keep other documents according to existing BSA and other recordkeeping requirements, including certain SEC rules that require six-year retention periods (*e.g.*, Exchange Act Rule 17a-4(a) requiring firms to preserve for a period of not less than six years, all records required to be retained by Exchange Act Rule 17a-3(a)(1)-(3), (a)(5), and (a)(21)-(22) and Exchange Act Rule 17a-4(e)(5) requiring firms to retain for six years account record information required pursuant to Exchange Act Rule 17a-3(a)(17)).

SAR Maintenance and Confidentiality

We will hold SARs and any supporting documentation confidential. We will not inform anyone outside of FinCEN, the SEC, a SRO registered with the SEC or other appropriate law enforcement or regulatory agency about a SAR. We will refuse any subpoena requests for SARs or for information that would disclose that a SAR has been prepared or filed and immediately notify FinCEN of any such subpoena requests that we receive.

We will segregate SAR filings and copies of supporting documentation from other firm books and records to avoid disclosing SAR filings. Our AML Compliance Person will handle all subpoenas or other requests for SARs.

We may share information with another financial institution about suspicious transactions in order to determine whether we will jointly file a SAR according to the provisions of Section 3.d. In cases in which we file a joint SAR for a transaction that has been handled both by us and another financial institution, both financial institutions will maintain a copy of the filed SAR.

Additional Records

We shall retain either the original or a microfilm or other copy or reproduction of each of the following:

- A record of each extension of credit in an amount in excess of $10,000, except an extension of credit secured by an interest in real property. The record shall contain the name and address of the person to whom the extension of credit is made, the amount thereof, the nature or purpose thereof and the date thereof;
- A record of each advice, request or instruction received or given regarding any transaction resulting (or intended to result and later canceled if such a record is normally made) in the transfer of currency or other monetary instruments, funds, checks, investment securities or credit, of more than $10,000 to or from any person, account or place outside the U.S.;
- A record of each advice, request or instruction given to another financial institution (which includes broker-dealers) or other person located within or without the U.S., regarding a transaction intended to result in the transfer of funds, or of currency, other monetary instruments, checks, investment securities or credit, of more than $10,000 to a person, account or place outside the U.S.;
- Each document granting signature or trading authority over each customer's account;
- Each record described in Exchange Act Rule 17a-3(a): (1) (blotters), (2) (ledgers for assets and liabilities, income, and expense and capital accounts), (3) (ledgers for cash and margin accounts), (4) (securities log), (5) (ledgers for securities in transfer, dividends and interest received, and securities borrowed and loaned), (6) (order tickets), (7) (purchase and sale tickets), (8) (confirms), and (9) (identity of owners of cash and margin accounts);
- A record of each remittance or transfer of funds, or of currency, checks, other monetary instruments, investment securities or credit, of more than $10,000 to a person, account or place, outside the U.S.; and

- A record of each receipt of currency, other monetary instruments, checks or investment securities and of each transfer of funds or credit, of more than $10,000 received on any one occasion directly and not through a domestic financial institution, from any person, account or place outside the U.S.

Clearing/Introducing Firm Relationships

We will work closely with our clearing firm to detect money laundering. We will exchange information, records, data and exception reports as necessary to comply [with our contractual obligations and] with AML laws. Both our firm and our clearing firm have filed (and kept updated) the necessary annual certifications for information sharing, which can be found on FinCEN's Web site. As a general matter, we will obtain and use the following exception reports offered by our clearing firm in order to monitor customer activity:

The AML Daily Detail Report, AMPS Fed Fund Third Party Activity Report, the Daily Money-line Report, and Wire Transfer Activity Report. Additionally, our clearing partners and our Firm have mutually agreed that the clearing entities will assume account activity review responsibilities as well as added support to our mutual AML program efforts.

We will provide our clearing firm with proper customer identification and due diligence information as required to successfully monitor customer transactions. We have discussed how each firm will apportion customer and transaction functions and how we will share information and set forth our understanding in a written document. We understand that the apportionment of functions will not relieve either of us from our independent obligation to comply with AML laws, except as specifically allowed under the BSA and its implementing regulations.

Training Programs

We will develop ongoing employee training under the leadership of the AML Compliance Person and senior management. Our training will occur on at least an annual basis. It will be based on our firm's size, its customer base, and its resources and be updated as necessary to reflect any new developments in the law.

Our training will include, at a minimum:

(1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties;

(2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, the filing of SARs);

(3) what employees' roles are in the firm's compliance efforts and how to perform them;

(4) the firm's record retention policy; and

(5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the BSA.

We will develop training in our firm, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos. Currently our training program is through FINRA's on-line e-Learning program regarding Anti- Money Laundering to be completed on an annual basis. We will maintain records to show the people trained, the dates of training and the subject matter of their training.

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

Program to Independently Test AML Program

Staffing

The testing of our AML program will be performed at least annually on a calendar year basis by an independent third party. We will evaluate the qualifications of the independent third party to ensure they have a working knowledge of applicable requirements under the BSA and its implementing regulations. Independent testing will be performed more frequently if circumstances are warranted. Our clearing partners' back-office system testing will be conducting periodically to ensure names are captured, hits are tracked in the back-office system and notated with any necessary documentation.

Evaluation and Reporting

After we have completed the independent testing, staff will report its findings to senior management. We will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved.

Monitoring Employee Conduct and Accounts

We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the AMLCO and their designated supervisor. We will also review the AML performance of supervisors, as part of their annual performance review.

Specific details of how the firm will monitor and supervise all other employees and registered representatives' conduct and accounts are detailed in the firm's Written Supervisory Procedures (WSPs).

Confidential Reporting of AML Non-Compliance

Employees will promptly report any potential violations of the firm's AML compliance program to the AML Compliance Person, unless the violations implicate the AML Compliance Person, in which case the employee shall report to the CEO. Such reports will be confidential, and the employee will suffer no retaliation for making them.

Additional Risk Areas

The firm has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above. After review and consideration, it is the opinion of Kingswood Capital, LLC that there exists no additional areas of risk with the duplicative AML efforts between our Firm and our Clearing Partners.

Updated IPO Red Flags Section
UPDATED IPO-SPECIFIC RED FLAGS SECTION

Red Flags Specific to Initial Public Offerings (IPOs)

In addition to the Firm's standard AML surveillance and red-flag indicators, Initial Public Offerings ("IPOs") present elevated risks of money laundering, market manipulation, nominee arrangements, undisclosed beneficial ownership, and illicit fund flows...

A. Issuer-Related Red Flags
• Unclear or implausible business purpose.
• Shell or newly formed issuer with limited operating history.
• Complex or opaque ownership structures.
• Sudden changes in directors or control persons.
• Promoters or intermediaries with adverse history.

B. Investor / Subscriber Red Flags
• Subscription amounts inconsistent with investor profile.
• Offshore or third-party funding sources.
• Refusal to disclose beneficial ownership.
• Indicators of nominee relationships.

C. Source-of-Funds Indicators
• Funds transmitted from high-risk jurisdictions.
• Circular or unexplained fund flows.
• Pooled or commingled accounts.

D. Market Activity Red Flags
• Coordinated or unusual post-IPO trading patterns.
• Price-support trading indicative of manipulation.
• Rapid liquidation by insiders without explanation.

E. Documentation & Due-Diligence Concerns
• Inconsistent or incomplete KYC/CDD documents.
• Discrepancies between issuer filings and representations.

F. Supervisory Requirements
• Perform issuer and subscriber due diligence.
• Apply EDD for high-risk scenarios.
• Document all escalations and SAR decisions.
• Maintain records under SEC Rule 17a-4.

G. Regulatory References

- FINRA Rule 3310
- 31 C.F.R. §1023.320
- FINRA Notice 10-22
- FINRA Regulatory Notice 22-25