Brighton Securities
Anti-Money Laundering (AML) Program:
Compliance and Supervisory Procedures

UPDATED AS OF January 2022

1. Firm Policy

It is the policy of Brighton Securities (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 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.

Although cash is rarely deposited into securities accounts, the securities industry is unique in that it can be used to launder funds obtained elsewhere, and to generate illicit funds within the industry itself through fraudulent activities. Examples of types of fraudulent activities include insider trading, market manipulation, Ponzi schemes, cybercrime and other investment-related fraudulent activity.

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.

Rules: 31 C.F.R. § 1023.210; FINRA Rule 3310.

2. AML Compliance Person Designation and Duties

The Firm has designated Lori Alberts as its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the firm's AML program. Lori Alberts has a working knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge and training. The duties of the AML Compliance Person will include monitoring the Firm's compliance with AML obligations, overseeing communication and training for employees, including the related Customer Identification Program ("CIP"). 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. Additionally, the AML Compliance person will monitor for new rules proposed under section 311 of the USA Patriot Act. They may do this by checking FINRA's AML webpage: http://www.finra.org/Industry/Issues/AML/index.htm.

The Firm will provide FINRA with contact information for the AML Compliance Person through the FINRA Contact System (FCS), including: (1) name; (2) title; (3) mailing address; (4) email address; (5) telephone number; and (6) facsimile (if any). 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 Lori Alberts 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, Lori Alberts will update the information promptly, but in any event not later than 30 days following the change.

Rules: 31 C.F.R. § 1023.210; FINRA Rule 3310; FINRA Rule 4517.
Resources: Regulatory Notice 07-42; NTM 06-07; NTM 02-78. Firms can submit their AML Compliance Person information through FINRA's FCS web page.

3. Giving AML Information to Federal Law Enforcement Agencies and Other Financial Institutions

a. FinCEN Requests Under USA PATRIOT Act Section 314(a)

The Firm 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 website. 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 are required to search those documents outlined in FinCEN's FAQ. If we find a match, Lori Alberts 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), Lori Alberts will structure our search accordingly.

If Lori Alberts searches our records and does not find a matching account or transaction, then Lori Alberts will not reply to the 314(a) Request. We will maintain documentation that we have performed the required search by printing the search self-verification document from FinCEN's 314(a) Secure Information Sharing System confirming that we have searched the 314(a) subject information against our records

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. Lori Alberts 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.

Rule: 31 C.F.R. § 1010.520.
Resources: FinCEN's 314(a) web page; NTM 02-80;. FinCEN also provides financial institutions with General Instructions and Frequently Asked Questions relating to 314(a) requests through the 314(a) Secured Information Sharing System or by contacting FinCEN's Regulatory Helpline at (800) 949-2732 or via email at sys314a@fincen.gov.

b. National Security Letters

National Security Letters (NSLs) are written investigative demands that may be issued by the local Federal Bureau of Investigation (FBI) 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.*** *If you file a Suspicious Activity Report (SAR) after receiving a NSL, the SAR should not contain any reference to the receipt or existence of the NSL.*

We understand that the receipt of a National Security Letter (NSL) is highly confidential. We understand that none of our officers, employees or agents may directly or indirectly disclose to any person that the FBI or other federal government authority has sought or obtained access to any of our records. To maintain the confidentiality of any NSL we receive, we will process and maintain the NSL by the CEO. If we file a SAR after receiving an NSL, the SAR will not contain any reference to the receipt or existence of the NSL. The SAR will only contain detailed information about the facts and circumstances of the detected suspicious activity.

Resource: *FinCEN SAR Activity Review, Trends, Tips & Issues, Issue 8 (National Security Letters and Suspicious Activity Reporting) (4/2005)*.

c. Grand Jury Subpoenas

We understand that the receipt of a grand jury subpoena concerning a customer, M&A client, or fund investor 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 individual or entity 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 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, Lori Alberts will process and maintain copies of any document related to the subpoena. 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.

Resources: *FinCEN SAR Activity Review, Trends, Tips & Issues, Issue 10 (Grand Jury Subpoenas and Suspicious Activity Reporting) (5/2006)*.

d. 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. Lori Alberts 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 website. 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:

- identifying and, where appropriate, reporting on money laundering or terrorist activities;

- determining whether to establish or maintain an account, or to engage in a transaction; or

- assisting the financial institution in complying with performing such activities.

Rules: 31 C.F.R. § 1010.540.
Resources: FinCEN Financial Institution Notification Form; FIN-2009-G002: Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act (6/16/2009).

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

We will file joint SARs in the following circumstances, according to an agreement with our clearing Firm under which the Firm is able to share some of its responsibilities pursuant to the Patriot Act and related regulations. Any such sharing should only be undertaken under the direction and control of the AML Compliance officer. The U.S. Treasury Interim Regulations require that the Firm file with the Treasury an annual Certification disclosing the sharing relationship and setting out the steps the Firm will take to protect the confidentiality of the shared information. The AML Compliance Officer is responsible for coordinating the flow of information and reporting between the firms in implementing the Firm's AML Program. 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 to 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.

Rules: 31 C.F.R. § 1023.320; 31 C.F.R. § 1010.430; 31 C.F.R. § 1010.540.
Resources: FinCEN's BSA E-Filing System.

4. Checking the Office of Foreign Assets Control Listings

Before opening an account, engaging in private placement or a transaction with a M&A client, and on an ongoing basis, Principal review of all new account documents, deal documents, or investor questionnaires, will include a check to ensure that a customer, client, or investor 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 website 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 and/or its clearing firm will also review existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated and will document the review.

If we determine that a customer, current client, or potential investor 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).

Rules: 31 C.F.R. § 501.603; 31 C.F.R. § 501.604.
Resources: SEC AML Source Tool for Broker-Dealers, Item 12; OFAC Lists web page (including links to the SDN List and lists of sanctioned countries); FINRA's OFAC Search Tool. You can also subscribe to receive updates on the OFAC Subscription web page. See also the following OFAC forms: Report of Blocked Transactions Form; Report of Rejected Transactions Form; Annual Report of Blocked Property Form; and OFAC Guidance Regarding Foreign Assets Control Regulations for the Securities Industry.

5. Customer Identification Program

In addition to the information we must collect under FINRA Rules 2090 (Know Your Customer) and 2111 (Suitability) and the 4510 Series (Books and Records Requirements), and Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3(a)(9) (Beneficial Ownership regarding Cash and Margin Accounts), 17a-3(a)(17) (Customer Accounts) and Regulation Best Interest, we have established, documented and maintained 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.

We will collect information to determine whether any entity opening an account would be excluded as a "customer," pursuant to the exceptions outlined in 31 CFR 1023.100(d)(2)) (*e.g.*, documentation of a company's listing information, licensing or registration of a financial institution in the U.S., and status or verification of the authenticity of a government agency or department).

Rule: 31 C.F.R. § 1023.220.
Resources: SEC Staff Q&A Regarding the Broker-Dealer Customer Identification Program Rule (10/1/2003); NTM 03-34.

a. Required Customer Information

Prior to opening an account or engaging in a private placement or M&A transaction, the Representative, Assistant, or appropriate staff member 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 or seeking to engage in an investment or transaction:

(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).

In the event that a customer has applied for, but has not received, a taxpayer identification number, we will await the tax identification number before opening an account or engaging in a transaction.

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.

Rule: 31 C.F.R. § 1023.220(a)(2)(i).

b. Customers Who Refuse to Provide Information

If a potential or existing customer, client or investor 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.

c. 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. Lori Alberts 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 identity when appropriate documents are available. In light of the 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, client, or potential investor. In verifying the information, we will consider whether the identifying information that we receive, such as 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, client or potential investor (*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 a 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 use the following non-documentary methods of verifying identity:

- 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 (e.g., Equifax);

- Checking references with other financial institutions; or

- Obtaining a financial statement.

We will use non-documentary methods of verification when:
(1) the customer, client, or potential investor 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, client, or potential investor and the 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 through documentary means.

We will verify the information within a reasonable time before or after the account is opened and before engaging in any transaction with a M&A client or potential investor. 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, client's or potential investor's true identity may be heightened for certain types of accounts and transactions, 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, clients, and potential investors 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, client, or potential investor when standard documentary methods prove to be insufficient: We also require the identification information for all parties who have authority or control over an account (e.g., Power of Attorney, Executor, etc.) in order for that account to remain in good standing.

Rule: 31 C.F.R. § 1023.220(a)(2)(ii).

d. Lack of Verification

When we cannot form a reasonable belief that we know the true identity of a customer, client, or potential investor 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 a customer's identity fail; and (4) determine whether it is necessary to file a SAR in accordance with applicable laws and regulations.

Rule: 31 C.F.R. § 1023.220(a)(2)(iii).

e. Recordkeeping

We will document our verification, including all identifying information provided by a customer, client, or potential investor, 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, client's, potential investor'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, client, or potential investor. 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.

Rule: 31 C.F.R. § 1023.220(a)(3).

f. 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.

Rule: 31 C.F.R. § 1023.220(a)(4).
Resource: NTM 02-21, page 6, n.24.

g. Notice to Customers

We will provide notice to customers, M&A clients, and potential investors 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: Prior to account opening, while obtaining new account data, the customer is verbally notified that we are requesting information from them in order to verify their identities.

h. 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:

- when such reliance is reasonable under the circumstances;
- 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

- 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.

Rule: 31 C.F.R. § 1023.220(a)(6).
Resources: No-Action Letters to the Securities Industry and Financial Markets Association (SIFMA) (February 12, 2004; February 10, 2005; July 11, 2006; January 10, 2008; January 11, 2010; January 11, 2011; January 9, 2015; December 12, 2016; and December 12, 2018)). (The letters provide staff guidance regarding the extent to which a broker-dealer may rely on an investment adviser to conduct the required elements of the CIP rule, prior to such adviser being subject to an AML rule.)

6. Customer Due Diligence Rule

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

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

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

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

The CDD Rule does not prescribe the form in which member firms must collect the required information, which includes the name, date of birth, address and Social Security number or other government identification number of beneficial owners. Rather, member firms may choose to obtain the information by using FinCEN's standard certification form in Appendix A of the CDD Rule (at https://www.fincen.gov/resources/filing-information) or by another means, provided that the chosen method satisfies the

identification requirements in the CDD Rule. In any case, the CDD Rule requires that member firms maintain records of the beneficial ownership information they obtain.

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

The CDD Rule's requirements with respect to beneficial owners of legal entity customers applies on a prospective basis, that is, only with respect to legal entity customers that open new accounts from the date of the CDD Rule's implementation. However, member firms should obtain beneficial ownership information for an existing legal entity customer if, during the course of normal monitoring, it receives information that is needed to assess or reevaluate the risk of the customer.

The required records to be created and maintained must include: (i) for identification, any identifying information obtained by the member firm pursuant to the beneficial ownership identification requirements of the CDD Rule, including without limitation the certification (if obtained); and (ii) for verification, a description of any document relied on (noting the type, any identification number, place of issuance and, if any, date of issuance and expiration), of any non-documentary methods and the results of any measures undertaken, and the resolution of each substantive discrepancy. In addition to complying with existing SEC and FINRA record retention requirements, member firms must maintain the records collected for identification purposes for a minimum of five years after the account is closed, and for verification purposes, for five years after the record is made.

Member firms may rely on the performance by another financial institution (including an affiliate) of the requirements of the CDD Rule with respect to any legal entity customer of the member firm that is opening, or has opened, an account or has established a similar business relationship with the other financial institution to provide or engage in services, dealings, or other financial transactions, provided that: (1) such reliance is reasonable under the circumstances; (2) the other financial institution is subject to a rule implementing 31 U.S.C. 5318(h) and is regulated by a Federal functional regulator; and (3) the other financial institution enters into a contract requiring it to certify annually to the member firm that it has implemented its AML program, and that it will perform (or its agent will perform) the specified requirements of the member firm's procedures to comply with the CDD Rule.

The CDD Rule also addresses the third and fourth components, which FinCEN states "are already implicitly required for covered financial institutions to comply with their

suspicious activity reporting requirements," by amending the existing AML program rules for covered financial institutions to explicitly require these components to be included in AML programs as a new "fifth pillar." These requirements are discussed further below.

Rules: 31 C.F.R. § 1010.230; 31 C.F.R. § 1023.210(b)(5); FINRA Rule 3310.
Resources: 81 Fed. Reg. 29398 (May 11, 2016) (Final Rule: Financial Crimes Enforcement Network; Customer Due Diligence Requirements for Financial Institutions); FIN-2016-G003: Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (7/19/2016); Regulatory Notice 17-40; FIN-2018-G001: Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (4/3/2018); Regulatory Notice 18-19.

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

a. Identification and Verification of Beneficial Owners

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

(1) the name;
(2) date of birth (for an individual);
(3) an address, which will be a residential or business street address (for an individual), or an Army Post Office (APO) or Fleet Post Office (FPO) box number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address); and
(4) an identification number, which will be a Social Security number (for U.S. persons), or one or more of the following: a passport number and country of issuance, or other similar identification number, such as an alien identification

[1] Beneficial owners and legal entity customers as defined by the CDD Rule.

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).

If your firm elects to utilize Appendix A to 31 CFR § 1010.230, record how the firm will use the document.

For verification, we will describe any document relied on (noting the type, any identification number, place of issuance and, if any, date of issuance and expiration). We will also describe any non-documentary methods and the results of any measures undertaken.

Rules: 31 C.F.R. § 1010.230(b); 31 C.F.R. § 1023.210(b)(5).
Resources: FIN-2016-G003: Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (7/19/2016); Regulatory Notice 17-40.

b. Understanding the Nature and Purpose of Customer Relationships

We will understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile through the following methods.

- *The type of customer;*
- *The account or service being offered;*
- *The customer's income;*
- *The customer's net worth;*
- *The customer's domicile;*
- *The customer's principal occupation or business; and*
- *In the case of existing customers, the customer's history of activity.*

Rules: 31 C.F.R. § 1010.230; 31 C.F.R. § 1023.210(b)(5)(i); FINRA Rule 3310.
Resources: FIN-2016-G003: Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (7/19/2016); Regulatory Notice 17-40; Regulatory Notice 18-19.

c. Conducting Ongoing Monitoring to Identify and Report Suspicious Transactions

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

Rules: 31 C.F.R. § 1010.230; 31 C.F.R. § 1023.210(b)(5)(ii); FINRA Rule 3310.

Resources: FIN-2016-G003: Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (7/19/2016); Regulatory Notice 17-40; Regulatory Notice 18-19.

7. Correspondent Accounts for Foreign Shell Banks

a. Detecting and Closing Correspondent Accounts of Foreign Shell Banks

The Firm does not establish, maintain, administer or manage correspondent accounts for foreign banks. The Firm does not enter into M&A engagements or act as private placement for foreign banks.

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

Rule: 31 C.F.R. § 1010.630; 31 C.F.R. § 1010.605.

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

a. Due Diligence for Correspondent Accounts of Foreign Financial Institutions

We have reviewed our accounts and we do not have, nor do we intend to open or maintain, correspondent accounts for foreign financial institutions. The AML Compliance Person and/or supervising Principal will scrutinize all new account documents during their review and prior to account acceptance in order to avoid opening such accounts.

Rule: 31 C.F.R. § 1010.610(a).

Resource: *FIN-2006-G009: Application of the Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to the Securities and Futures Industries (5/10/2006)*.

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

We do not open or maintain private banking accounts.

Rule: *31 C.F.R. § 1010.620.*
Resources: *Guidance on Enhanced Scrutiny for Transactions that May Involve the Proceeds of Foreign Official Corruption (1/1/2001)*; *FIN-2008-G005: Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Political Corruption (4/17/2008)*.

10. 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.

Rules: *31 C.F.R. §§ 1010.651, 1010.653, 1010.655, 1010.658, 1010.659, 1010.660.*
Resources: *Section 311 – Special Measures (for information on all special measures issued by FinCEN); NTM 07-17; NTM 06-41*.

11. Monitoring Accounts for Suspicious Activity

We will monitor customer account, M&A client, and investor 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 continuously through a manual review process and should attempt to identify if a customer, M&A client, or potential investor:

- exhibits usual unease at government reporting requirements
- is reluctant to reveal data as to business activities, source of funds, etc.
- wishes to engage in transactions lacking business sense or demonstrable connection to the customer's, client's, or potential investor's other activities

- identifies a source of funds or securities that is false, misleading or substantially incorrect
- refuses to identify the source of funds or securities
- has a questionable background
- has an overseas address with P.O. Box number
- opens an account or funds a transaction with a "third party" check
- appears to be acting for an undisclosed principal or "family" or other unnamed person(s) and refuses to identify them
- has difficulty in describing his or her business or lacks general knowledge of his or her industry
- plans to engage in an unusual or complex transaction or one which he or she cannot clearly explain or involving parties not fully disclosed
- engages in transactions under $10,000 or which otherwise appear to be deigned to evade government reporting requirements.
- makes frequent currency or cash equivalent deposits, insists in dealing only in very liquid securities
- engages in multiple transfers of funds or securities in and out of "tax haven" or other secrecy jurisdictions
- has sudden extensive wire or check transaction activity without apparent business purpose
- has account activity or transaction size does not reconcile with stated net worth or investment objectives
- deposits funds, then requires all or part be immediately wired out
- bounces checks
- deposits funds to make a long term investment, thereafter liquidates it and transfers the money out
- maintains multiple accounts under a single name or related names with many inter-account transfers
- engages in excessive journal entries among unrelated accounts with no apparent business purpose
- requires that a transaction be processed so as to avoid the Firm's normal documentation requirements
- traffics in Regulation "S" stocks, bearer bonds and other securities known to be used for money laundering
- seems oblivious to commissions, transaction charges, etc. or
- deposits bearer bonds followed by an immediate request for liquidation and disbursement of the proceeds.

The customer risk profile will serve as a baseline for assessing potentially suspicious activity. The AML Compliance Person or his or her designee in consultation with the CEO of the Firm, 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.

We will document our monitoring and reviews in the files kept by the AML Compliance Person. The AML Compliance Person or his or her designee will conduct an appropriate investigation and review relevant information from internal or third-party sources before a SAR is filed. Relevant information can include, but not limited to, the following: "Account Opening Stage" and "Account Activity"

Rules: 31 C.F.R. § 1023.320; FINRA Rule 3310.
Resource: 67 Fed. Reg. 44048 (July 1, 2002) (Final Rule: Financial Crimes Enforcement Network; Amendment to the Bank Secrecy Act Regulations – Requirement that Brokers or Dealers in Securities Report Suspicious Transactions) it is intended that broker-dealers, and indeed every type of financial institution to which the suspicious transaction reporting rules of 31 CFR part 103 apply, will evaluate customer activity and relationships for money laundering risks, and design a suspicious transaction monitoring program that is appropriate for the particular broker-dealer in light of such risks").

a. 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, client, or potential investor 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 ((585) 263-6760*)*, local FBI office ((585) 546-220*)* and local SEC office ((877) 442-0854) (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 a 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.

Rule: 31 C.F.R. § 1023.320.
Resources: FinCEN's website; OFAC web page; NTM 02-21; NTM 02-47.

b. Red Flags

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

Potential Red Flags in Customer Due Diligence and Interactions with Customers

- The customer provides the firm with unusual or suspicious identification documents that cannot be readily verified or are inconsistent with other statements or documents that the customer has provided. Or, the customer provides information that is inconsistent with other available information about the customer. This indicator may apply to account openings and to interaction subsequent to account opening.
- The customer is reluctant or refuses to provide the firm with complete customer due diligence information as required by the firm's procedures, which may include information regarding the nature and purpose of the customer's business, prior financial relationships, anticipated account activity, business location and, if applicable, the entity's officers and directors.
- The customer refuses to identify a legitimate source of funds or information is false, misleading or substantially incorrect.
- The customer is domiciled in, doing business in or regularly transacting with counterparties in a jurisdiction that is known as a bank secrecy haven, tax shelter, high-risk geographic location (*e.g.*, known as a narcotics producing jurisdiction, known to have ineffective AML/Combating the Financing of Terrorism systems) or conflict zone, including those with an established threat of terrorism.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer has no discernable reason for using the firm's service or the firm's location (*e.g.*, the customer lacks roots to the local community or has gone out of his or her way to use the firm).
- The customer has been rejected or has had its relationship terminated as a customer by other financial services firms.
- The customer's legal or mailing address is associated with multiple other accounts or businesses that do not appear related.
- The customer appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.
- The customer is a trust, shell company or private investment company that is reluctant to provide information on controlling parties and underlying beneficiaries.
- The customer is publicly known or known to the firm to have criminal, civil or regulatory proceedings against him or her for crime, corruption or misuse of public funds, or is known to associate with such persons. Sources for this information could include news items, the Internet or commercial database searches.
- The customer's background is questionable or differs from expectations based on business activities.
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, with no apparent business or other purpose.
- An account is opened by a politically exposed person (PEP),[9] particularly in conjunction with one or more additional risk factors, such as the account being opened by a shell company[10] beneficially owned or controlled by the PEP, the PEP is

from a country which has been identified by FATF as having strategic AML regime deficiencies, or the PEP is from a country known to have a high level of corruption.

- An account is opened by a non-profit organization that provides services in geographic locations known to be at higher risk for being an active terrorist threat.[11]
- An account is opened in the name of a legal entity that is involved in the activities of an association, organization or foundation whose aims are related to the claims or demands of a known terrorist entity.[12]
- An account is opened for a purported stock loan company, which may hold the restricted securities of corporate insiders who have pledged the securities as collateral for, and then defaulted on, purported loans, after which the securities are sold on an unregistered basis.
- An account is opened in the name of a foreign financial institution, such as an offshore bank or broker-dealer, that sells shares of stock on an unregistered basis on behalf of customers.
- An account is opened for a foreign financial institution that is affiliated with a U.S. broker-dealer, bypassing its U.S. affiliate, for no apparent business purpose. An apparent business purpose could include access to products or services the U.S. affiliate does not provide.

Potential Red Flags in Deposits of Securities

- A customer opens a new account and deposits physical certificates, or delivers in shares electronically, representing a large block of thinly traded or low-priced securities.
- A customer has a pattern of depositing physical share certificates, or a pattern of delivering in shares electronically, immediately selling the shares and then wiring, or otherwise transferring out the proceeds of the sale(s).
- A customer deposits into an account physical share certificates or electronically deposits or transfers shares that:
  - were recently issued or represent a large percentage of the float for the security;
  - reference a company or customer name that has been changed or that does not match the name on the account;
  - were issued by a shell company;
  - were issued by a company that has no apparent business, revenues or products;
  - were issued by a company whose SEC filings are not current, are incomplete, or nonexistent;
  - were issued by a company that has been through several recent name changes or business combinations or recapitalizations;
  - were issued by a company that has been the subject of a prior trading suspension; or
  - were issued by a company whose officers or insiders have a history of regulatory or criminal violations, or are associated with multiple low-priced stock issuers.

- The lack of a restrictive legend on deposited shares seems inconsistent with the date the customer acquired the securities, the nature of the transaction in which the securities were acquired, the history of the stock or the volume of shares trading.

- A customer with limited or no other assets at the firm receives an electronic transfer or journal transfer of large amounts of low-priced, non-exchange-listed securities.

- The customer's explanation or documents purporting to evidence how the customer acquired the shares does not make sense or changes upon questioning by the firm or other parties. Such documents could include questionable legal opinions or securities purchase agreements.

- The customer deposits physical securities or delivers in shares electronically, and within a short timeframe, requests to journal the shares into multiple accounts that do not appear to be related, or to sell or otherwise transfer ownership of the shares.

- Seemingly unrelated clients open accounts on or at about the same time, deposit the same low-priced security and subsequently liquidate the security in a manner that suggests coordination.

Potential Red Flags in Securities Trading

- 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, which 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.)

- There is a sudden spike in investor demand for, coupled with a rising price in, a thinly traded or low-priced security.

- The customer's activity represents a significant proportion of the daily trading volume in a thinly traded or low-priced security.

- A customer buys and sells securities with no discernable purpose or circumstances that appear unusual.

- Individuals known throughout the industry to be stock promoters sell securities through the broker-dealer.

- A customer accumulates stock in small increments throughout the trading day to increase price.

- A customer engages in pre-arranged or other non-competitive securities trading, including wash or cross trades, with no apparent business purpose.

- A customer attempts to influence the closing price of a stock by executing purchase or sale orders at or near the close of the market.

- A customer engages in transactions suspected to be associated with cyber breaches of customer accounts, including potentially unauthorized disbursements of funds or trades.

- A customer engages in a frequent pattern of placing orders on one side of the market, usually inside the existing National Best Bid or Offer (NBBO), followed by the customer entering orders on the other side of the market that execute against other market participants that joined the market at the improved NBBO (activity indicative of "spoofing").

- A customer engages in a frequent pattern of placing multiple limit orders on one side of the market at various price levels, followed by the customer entering orders on the opposite side of the market that are executed and the customer cancelling the original limit orders (activity indicative of "layering").

- Two or more unrelated customer accounts at the firm trade an illiquid or low-priced security suddenly and simultaneously.

- The customer makes a large purchase or sale of a security, or option on a security, shortly before news or a significant announcement is issued that affects the price of the security.

- The customer is known to have friends or family who work at or for the securities issuer, which may be a red flag for potential insider trading or unlawful sales of unregistered securities.

- The customer's purchase of a security does not correspond to the customer's investment profile or history of transactions (*e.g.*, the customer may never have invested in equity securities or may have never invested in a given industry, but does so at an opportune time) and there is no reasonable explanation for the change.

- The account is using a master/sub structure, which enables trading anonymity with respect to the sub-accounts' activity, and engages in trading activity that raises red flags, such as the liquidation of microcap issuers or potentially manipulative trading activity.

- The firm receives regulatory inquiries or grand jury or other subpoenas concerning the firm's customers' trading.

- The customer engages in a pattern of transactions in securities indicating the customer is using securities to engage in currency conversion. For example, the customer delivers in and subsequently liquidates American Depository Receipts (ADRs) or dual currency bonds for U.S. dollar proceeds, where the securities were originally purchased in a different currency.

- The customer engages in mirror trades or transactions involving securities used for currency conversions, potentially through the use of offsetting trades.

- The customer appears to buy or sell securities based on advanced knowledge of pending customer orders.

Potential Red Flags in Money Movements

- The customer attempts or makes frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies and procedures relating to the deposit of cash and cash equivalents.

- The customer "structures" deposits, withdrawals or purchases of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements, and may state directly that they are trying to avoid triggering a reporting obligation or to evade taxing authorities.

- The customer seemingly breaks funds transfers into smaller transfers to avoid raising attention to a larger funds transfer. The smaller funds transfers do not appear to be based on payroll cycles, retirement needs, or other legitimate regular deposit and withdrawal strategies.

- The customer's account shows numerous currency, money order (particularly sequentially numbered money orders) or cashier's check transactions aggregating to significant sums without any apparent business or lawful purpose.

- The customer frequently changes bank account details or information for redemption proceeds, in particular when followed by redemption requests.

- 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.

- Wire transfers are made in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

- Incoming payments are made by third-party checks or checks with multiple endorsements.

- Outgoing checks to third parties coincide with, or are close in time to, incoming checks from other third parties.

- Payments are made by third party check or money transfer from a source that has no apparent connection to the customer.

- Wire transfers are made to or from financial secrecy havens, tax havens, high-risk geographic locations or conflict zones, including those with an established presence of terrorism.

- Wire transfers originate from jurisdictions that have been highlighted in relation to black market peso exchange activities.

- The customer engages in transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (*e.g.*, countries designated by national authorities, such as FATF, as non-cooperative countries and territories).

- The parties to the transaction (*e.g.*, originator or beneficiary) are from countries that are known to support terrorist activities and organizations.

- Wire transfers or payments are made to or from unrelated third parties (foreign or domestic), or where the name or account number of the beneficiary or remitter has not been supplied.

- There is wire transfer activity that is unexplained, repetitive, unusually large, shows unusual patterns or has no apparent business purpose.

- The securities account is used for payments or outgoing wire transfers with little or no securities activities (*i.e.*, account appears to be used as a depository account or a conduit for transfers, which may be purported to be for business operating needs).

- Funds are transferred to financial or depository institutions other than those from which the funds were initially received, specifically when different countries are involved.

- The customer engages in excessive journal entries of funds between related or unrelated accounts without any apparent business purpose.

- The customer uses a personal/individual account for business purposes or vice versa.

- A foreign import business with U.S. accounts receives payments from outside the area of its customer base.

- There are frequent transactions involving round or whole dollar amounts purported to involve payments for goods or services.

- Upon request, a customer is unable or unwilling to produce appropriate documentation (*e.g.*, invoices) to support a transaction, or documentation appears doctored or fake (*e.g.*, documents contain significant discrepancies between the descriptions on the transport document or bill of lading, the invoice, or other documents such as the certificate of origin or packing list).

- The customer requests that certain payments be routed through nostro[14] or correspondent accounts held by the financial intermediary instead of its own accounts, for no apparent business purpose.

- Funds are transferred into an account and are subsequently transferred out of the account in the same or nearly the same amounts, especially when the origin and destination locations are high-risk jurisdictions.

- A dormant account suddenly becomes active without a plausible explanation (*e.g.*, large deposits that are suddenly wired out).

- Nonprofit or charitable organizations engage in financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.

- There is unusually frequent domestic and international automated teller machine (ATM) activity.

- A person customarily uses the ATM to make several deposits into a brokerage account below a specified BSA/AML reporting threshold.

- Many small, incoming wire transfers or deposits are made using checks and money orders that are almost immediately withdrawn or wired out in a manner inconsistent with the customer's business or history; the checks or money orders may reference in a memo section "investment" or "for purchase of stock." This may be an indicator of a Ponzi scheme or potential funneling activity.

- Wire transfer activity, when viewed over a period of time, reveals suspicious or unusual patterns, which could include round dollar, repetitive transactions or circuitous money movements.

Potential Red Flags in Insurance Products

- The customer cancels an insurance contract and directs that the funds be sent to a third party.

- The customer deposits an insurance annuity check from a cancelled policy and immediately requests a withdrawal or transfer of funds.

- The customer cancels an annuity product within the free-look period. This could be a red flag if accompanied with suspicious indicators, such as purchasing the annuity with several sequentially numbered money orders or having a history of cancelling annuity products during the free-look period.

- The customer 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.

- The customer purchases an insurance product with no concern for the investment objective or performance.

Other Potential Red Flags

- The customer is reluctant to provide information needed to file reports to proceed with the transaction.

- The customer exhibits unusual concern with the firm's compliance with government reporting requirements and the firm's AML policies.

- The customer tries to persuade an employee not to file required reports or not to maintain the required records.

- Notifications received from the broker-dealer's clearing firm that the clearing firm had identified potentially suspicious activity in customer accounts. Such notifications can take the form of alerts or other concern regarding negative news, money movements or activity involving certain securities.

- Law enforcement has issued subpoenas or freeze letters regarding a customer or account at the securities firm.

- The customer makes high-value transactions not commensurate with the customer's known income or financial resources.

- The customer wishes to engage in transactions that lack business sense or an apparent investment strategy, or are inconsistent with the customer's stated business strategy.

- The stated business, occupation or financial resources of the customer are not commensurate with the type or level of activity of the customer.

- The customer engages in transactions that show the customer is acting on behalf of third parties with no apparent business or lawful purpose.

- The customer engages in transactions that show a sudden change inconsistent with normal activities of the customer.

- Securities transactions are unwound before maturity, absent volatile market conditions or other logical or apparent reason.

- The customer does not exhibit a concern with the cost of the transaction or fees (*e.g.*, surrender fees, or higher than necessary commissions).

- A borrower defaults on a cash-secured loan or any loan that is secured by assets that are readily convertible into currency.

- There is an unusual use of trust funds in business transactions or other financial activity.

Resource: *Regulatory Notice 19-18*

c. 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 AML Compliance Person. If the AML Compliance Person is unavailable the employee will notify a Supervising Principal. 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.

12. Suspicious Transactions and BSA Reporting

a. 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:

(1) 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;
(2) the transaction is designed, whether through structuring or otherwise, to evade any requirements of the BSA regulations;
(3) 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
(4) 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-SF 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-SF. 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.

Rules: 31 C.F.R. § 1023.320; FINRA Rule 3310.
Resources: FinCEN's website contains additional information, including information on the BSA E-Filing System, the FinCEN Suspicious Activity Report: Introduction and Filing Instructions, and the biannual SAR Activity Review – Trends, Tips & Issues, which discusses trends in suspicious reporting and gives helpful tips; The SAR Activity Review, Issue 10 (May 5/2006) (documentation of decision not to file a SAR; grand jury subpoenas and suspicious activity reporting, and commencement of 30-day time period to file a SAR); FinCEN SAR Narrative Guidance Package (11/2003), FinCEN Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting (10/10/2007); NTM 02-21; NTM 02-47.

b. Currency Transaction Reports

Our Firm prohibits transactions involving currency and has the following procedures to prevent such transactions: the Firm prohibits any employee from accepting currency. 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 *BSA E-Filing System* to file the supported CTR Form.

Rules: 31 C.F.R. §§ 1010.311, 1010.306, 1010.312.
Resource: FinCEN's BSA E-Filing System (including instructions for FinCEN CTR Form 112).

c. 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 website.

Rules: 31 C.F.R. §§ 1010.340, 1010.306.
Resources: FinCEN's BSA E-Filing System.

d. Foreign Bank and Financial Accounts Reports

We will file a Foreign Bank and Financial Accounts Report (FBAR) 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 BSA E-Filing System provided on FinCEN's website.

Rules: 31 C.F.R. §§ 1010.306, 1010.350, 1010.420.
Resources: FinCEN's BSA E-Filing System.

e. Monetary Instrument Purchases

We do not issue bank checks or drafts, cashier's checks, money orders or traveler's checks.

Rule: 31 C.F.R. § 1010.415.
Resource: 59 Fed. Reg. 52250 (October 17, 1994) (Final Rule; Amendments to BSA Regulations Relating to Identification Required to Purchase Bank Checks and Drafts, Cashier's Checks, Money Orders, and Traveler's Checks).

f. 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.

Rules: 31 C.F.R. § 1010.410(e) and (f); Exchange Act Rule 17a-8 (requiring registered broker-dealers subject to the Currency and Foreign Transactions Reporting Act of 1970 to comply with the BSA regulations regarding reporting, recordkeeping and record retention requirements); FINRA Rule 3310.

13. AML Recordkeeping

a. 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)).

Rules: 31 C.F.R. § 1010.430; Exchange Act Rule 17a-8 (requiring registered broker-dealers subject to the Currency and Foreign Transactions Reporting Act of 1970 to comply with the BSA regulations regarding reporting, recordkeeping and record retention requirements); FINRA Rule 3310.

b. SAR Maintenance and Confidentiality

We will hold SARs and any supporting documentation confidential. We will not inform anyone outside of FinCEN, the SEC, an 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. *See* Section 11 for contact numbers. 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.

Rule: 31 C.F.R. § 1023.320(e).
Resources: 67 Fed. Reg. 44048 (July 1, 2002) (Final Rule; Financial Crimes Enforcement Network; Amendment to the Bank Secrecy Act Regulations – Requirement that Brokers or Dealers in Securities Report Suspicious Transactions); NTM 02-47.

c. 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.

Rules: 31 C.F.R. § 1010.410; 31 C.F.R. 1023.410; Exchange Act Rule 17a-8 (requiring registered broker-dealers subject to the Currency and Foreign Transactions Reporting Act of 1970 to comply with the BSA regulations regarding reporting, recordkeeping and record retention requirements); FINRA Rule 3310.

Rules: 31 C.F.R. § 1010.410; 31 C.F.R. 1023.410; Exchange Act Rule 17a-8 (requiring registered broker-dealers subject to the Currency and Foreign Transactions Reporting Act of 1970 to comply with the BSA regulations regarding reporting, recordkeeping and record retention requirements); FINRA Rule 3310.

14. 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 such information sharing, which can be found on FinCEN's website. As a general matter, we will obtain and use the following exception reports offered by our clearing firm in order to monitor customer activity: AML: ACH Transactions Report, Checks Report, Deposits Report, Fed Wire Report, Securities Receives Report, DAML Owner Addition Confirmation Report, Name/Address Change Confirmation Report, BRR-No DAML Report,

Unsecured Debits – Weekly (IRA & Non IRA), Investment Objective Change Report, No DAML Report, and Cash Due – Trade Settles Report. These reports are reviewed daily and/or weekly where noted to assist in the review of customer accounts for, among other reasons, red flags, or suspicious activity and 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.

Rules: 31 CFR § 1010.540; FINRA Rule 3310; FINRA Rule 4311.
Resource: NTM 02-21.

15. 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, client, and investor 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: all covered persons must complete annual AML training delivered as part of the Firm Element of Continuing Education, a component of the Annual Compliance Meeting, or both. We will maintain records to show the persons 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.

Rules: 31 CFR § 1023.210(b)(4); FINRA Rule 3310.
Resources: See NTM 02-21, FinCEN SAR Narrative Guidance Package (11/01/2003); FinCEN Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting (10/10/2007).

16. Program to Independently Test AML Program

a. Staffing

The testing of our AML program will be performed at least annually (on a calendar year basis) by member personnel or the CPA firm of RDG + Partners, an independent third party or David Manicoci, Certified Public Accountant. We will evaluate the qualifications of said member personnel or the independent third party to ensure they have a working knowledge of applicable requirements under the BSA and its implementing regulations. Member personnel and RDG + Partners are members of the American Institute of Certified Public Accountants (AICPA) and the New York State Society of Certified Public Accountants (NYSSCPA). Independent testing will be performed more frequently if circumstances warrant.

Rules: 31 C.F.R. § 1023.210(b)(2); FINRA Rule 3310.
Resource: NTM 06-07.

b. 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.

Rules: 31 C.F.R. § 1023.210(b)(2); FINRA Rule 3310.

17. Monitoring Employee Conduct and Accounts

We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the AML Compliance Person. We will also review the AML performance of supervisors, as part of their annual performance review. The AML Compliance Person's accounts will be reviewed by Jai Ramachandran, CEO.

Rules: 31 C.F.R. § 1023.320; 31 C.F.R § 1023.210; FINRA Rule 3310.

18. 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.

Rules: 31 C.F.R. § 1023.210; FINRA Rule 3310.

19. 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. The major additional areas of risk include transactions taking place in direct business products such as annuities or mutual funds held directly at the fund. It is incumbent on the branch office manager, supervising Principal, and AML Compliance Person to apply these procedures to those transactions as well as all others.

20. Senior Manager Approval

Senior management has approved this AML compliance program in writing as reasonably designed to achieve and monitor our Firm's ongoing compliance with the requirements of the BSA and the implementing regulations under it. This approval is indicated by signatures below.

Rules: *31 C.F.R. § 1023.210; FINRA Rule 3310.*

Signed:

Title:

Date: