Anti-Money Laundering Policies & Procedures Manual

Introduction

It is the policy of this 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 this firm as enacted, as well as the applicable requirement under the Bank Secrecy Act ("BSA"). This manual will provide a basic understanding of the Firm's policies and procedures. As an IAR you agree to attend all webinars and our annual compliance meetings, so you have a thorough knowledge of all aspect of money laundering.

Money laundering is 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 regularly 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.

Anti-Money Laundering Policies

The Firm has designated its Chief Compliance Officer and Compliance Consultant as the department to oversee, educate, and monitor all aspects of money laundering. It will be this department's responsibility to assure that its policies and procedures are being followed. As such, this department will be empowered by the Firm with full responsibility and authority to develop and enforce appropriate AML

policies and procedures. Further, it will be this department's responsibility to update and keep current such AML policies and procedures. All updates will be posted on the Firm's website. The Firm, or any of its IARs as a matter of policy, will not be party to any transaction and will not facilitate any transaction with any person(s) or entity(ies) (Prohibited Person) listed on the web site maintained by the Office of Foreign Assets Control (www.treas.gov/ofac) relating thereto. If the AML compliance officer learns that any Prohibited Person is, or is attempting to become, involved in any transaction concerning the services which the Advisor provides, the AML compliance officer shall immediately report such transaction to the Office of Foreign Assets Control.

The Firm has established basic policies to comply with the BSA. Below is an outline of the Firm's policies according to the BSA.

1. Establish and implement policies, procedures, and internal controls reasonably designed to prevent the Advisor from being used to launder money or finance terrorist activities, including but not limited to achieving compliance with applicable provisions of the Bank Secrecy Act (BSA) and the Financial Crimes Enforcement Network's (FinCEN) implementing regulations and the AML regulations of other countries and jurisdictions with authority over any transaction to which the Advisor is a party. The AML compliance officer will review the types of services the Advisor provides and the nature of its clients to identify the Advisor's vulnerability to any money laundering activities. The AML compliance officer will, after such review, develop and implement policies and procedures that would reasonably address such issues and periodically assess the effectiveness of such policies and procedures.

2. Provide for independent testing of compliance with the Advisor's AML policies and procedures. The testing of these policies and procedures will be conducted at least annually by Advisor personnel or by a qualified outside third party. A written assessment of the Advisor's AML policies should be generated, reviewed by the AML compliance officer and filed in the AML policy folder. Any recommendations resulting from such review should be promptly addressed.

3. Provide, at least annually, training for any employee involved in managing client assets. The AML compliance officer will create a list of these individuals. These employees will be made aware of BSA requirements relevant to their functions and trained in recognizing possible signs of money laundering that could arise in the course of their duties. The AML compliance officer will evaluate the effectiveness of such training programs and adjust the program(s) offered as needed. Further, the AML compliance officer will document such training sessions by recording the names of those individuals attending and the dates of attendance.

4. Report suspicious activity to the appropriate government officials when, in the opinion of the AML compliance officer, such reporting is required under applicable law.

Anti-Money Laundering Procedures

These procedures are divided into three parts: (1) Account Opening and Ongoing Client Account Activity, (2) Education and Training, and (3) Books and Records.

Account Opening and Ongoing Account Activity

In addition to the information required by the Account Application, sponsor and/or other forms, the Firm's IARs should be alert to the following "Red Flags":

- The client exhibits unusual concern for secrecy, particularly concerning his identity, type of business, assets or dealings with firms, or the client provides non-verifiable references or is reluctant or refuses to provide financial information or information concerning financial relationships and business activities.
- The client exhibits a lack of concern regarding risks, advisory fees, commissions, or other transaction costs. Upon request, the client refuses to identify or fails to indicate a legitimate source for his funds and other assets.
- The client appears to operate as an agent for an undisclosed principal but is reluctant to provide information regarding that entity. Beneficial ownership is difficult to ascertain.
- The client has difficulty describing the nature of his business or lacks general knowledge of his industry.
- The client is from or has accounts in, a country identified as a haven for money laundering.
- The client, or a person publicly associated with the client, has a questionable background, including prior criminal convictions.
- A client attempts to open an account with unusual or suspect identification or business documents.
- The opening of an account for a client who is more interested in writing checks and utilizing a debit card than investing.

Lack of Verification Policy

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

Personal Accounts

For each new client (and especially for walk-in clients, foreign clients or clients wanting to open an account with a foreign address), the IAR will take reasonable steps to determine the client's true identity. Various steps can include: (i) Requiring satisfactory identification to corroborate client's identity (e.g., a driver's license with a photo, a U.S. passport, or alien registration card); (ii) Obtaining basic background information on client, such as residence and/or place of business; (iii) Considering the proximity of client's residence or place of business to branch location and, if it is inconvenient, determine why client is opening an account at that location; (iv) Obtaining information on client's source of funds to open the account and investigate the source of funds of large deposits; (v) Calling client's residence or place of employment to thank him or her for opening the account and further investigate any suspicious responses, including disconnected phone service or no record of employment; and (vi) Considering use of third party references (e.g., credit bureau, verification service, or telephone and web site directories).

Business Accounts

For each new client (and especially for walk-in clients, foreign clients and clients wanting to open an account with a foreign address), the IAR must take reasonable steps to verify the identity of the agent of the business and the beneficial owners of the business.

Various steps can include: (i) Verifying legal status of business (e.g., sole proprietorship, partnership, incorporation or association); (ii) determining beneficial owners of business; (iii) Checking name of business with information-reporting agencies and check prior bank references; (iv) Calling client's business to thank him or her for opening the account and investigate unusual circumstances, such as disconnected phone service; (v) Verifying that business exists and is conducting its stated activities, if appropriate, by visiting the business; (vi) Considering source of funds used to open account and investigate large deposits; (vii) Consideration of obtaining: a financial statement; description of client's principal line of business or primary trade area; description of business operations, anticipated volume of cash and total sales, and list of major clients; and a third-party reference.

High-Risk Business Entities

The following types of businesses have been identified by regulators as being at a higher risk to money laundering activities: (i) Nontraditional financial entities such as currency exchange houses, money transmitters, and check cashing facilities; (ii) Casinos and card clubs; (iii) Offshore corporations and banks located in tax and/or secrecy havens; (iv) Leather goods stores; (v) Car, boat, and plane dealerships; (vi) Used automobile or truck dealers and machine parts manufacturers; (vii) Travel agencies; (viii) Jewel, gem, and precious metal dealers; (ix) Import/export companies; (x) Auctioneers; (x) Deposit brokers; (xi) Pawnbrokers; (xii) Professional service providers (e.g., lawyers, accountants, investment brokers); (xiii) Cash-intensive businesses, such as convenience stores, restaurants, retail stores, and parking garages; (xiv) Ship, bus, and plane operators; (xv) Telemarketers.

Pre-Approval Required for Opening of Certain New Accounts. The IAR shall contact Mr. McBroom, CCO regarding any person or entity who is a citizen of or resides in the identified high-risk countries set forth above or is associated in any way with the listed individuals or entities referenced in those sections, before opening an account for such person or entity. The IAR can also independently research this information by visiting the FATF, FinCEN or OFAC websites.

Supplemental Documentation

Advisor reserves the right to request supplemental documentation from certain new, existing, and prospective accounts, including, but not limited to audited financial statements, copies of tax returns, employment representations, and verifications, credit reports, non-resident alien client profile forms, banking verifications, any documentation requested by the clearing firm, and general due diligence questionnaires.

Other Policies Involving AML Information to Federal Law Enforcement Agencies and Other Financial Institutions

FinCEN Requests under USA PATRIOT Act Section 314(a)

The Firm and any IARs 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, [Name] 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), [Name] will structure our search accordingly.

The Firm will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. The Firm's AML department 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.

The Firm 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, the Firm 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.*

National Security Letters

The Firm understands that the receipt of a National Security Letter (NSL) is highly confidential. The Firm understands 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, the Firm will process and maintain the NSL by uploading any documentation to a secure and encrypted location or file. If the Firm files 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).*

Grand Jury Subpoenas

The Firm understands that the receipt of a grand jury subpoena concerning a customer does not in itself require that we file a Suspicious Activity Report (SAR). When the Firm receives a grand jury subpoena, our AML department will conduct a risk assessment of the customer subject to the subpoena as well as review the customer's account activity. If we uncover suspicious activity during our risk assessment and review, we will elevate that customer's risk assessment and file a SAR in accordance with the SAR filing requirements. We understand that none of our officers, employees or agents may directly or indirectly disclose to the person who is the subject of the subpoena its existence, its contents or the information we used to respond to it. To maintain the confidentiality of any grand jury subpoena we receive, we will process and maintain the subpoena by copy and uploading the subpoenas into an encrypted PDF file and maintain such records in a secure folder. If our AML department files 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).*

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

Our AML department will share information with other financial institutions regarding individuals, entities, organizations, and countries for purposes of identifying and, where appropriate, reporting activities that it suspects may involve possible terrorist activity or money laundering. Our AML department 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 on FinCEN's website. Before this department shares information with another financial institution, it 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.

Recording Keeping

The Firm will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. Concerning 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. The Firm will also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information ob-

tained. 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. Our AML department will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information by segregating it from the firm's other books and records.

Rule: *31 C.F.R. § 1023.220(a)(3). 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).*