

REMITANO

Anti-Money Laundering (AML) Policy

UPDATED AS OF NOVEMBER 30TH, 2022

1. General Policy

This is the policy of Remitano (hereinafter as 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 applicable requirements under the FATF Recommendations 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 crypto accounts, the crypto 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.

Our AML policies, procedures and internal controls have been designed to ensure compliance with applicable FATF Recommendations and shall 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.

2. Reporting AML Information to National Law Enforcement Agencies and Other Financial Institutions

We shall respond to any National Law Enforcement Agencies request concerning accounts' credentials and transactions 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 blacklisted or sanctioned. We understand that we have 14 days from the transmission date of the request to respond. We will designate one or more persons to be the point of contact (POC) for Requests and will promptly update the POC information following any change in such information. In case of suspecting or having reasonable grounds to suspect that

funds or transactions are the process of criminal activity, or are related to terrorist financing, our AML Compliance Officer shall promptly report to the person submitting the request through the system they sent us 14 days or within the time period they specify. If our AML Compliance Officer searches our records and does not find a matching account's credential or transaction, then we will not reply to their Request. We will maintain documentation that we have performed the required.

We will not disclose the fact that anyone has requested or obtained information from us, except to the extent necessary to comply with the information request. Our AML Compliance Officer will review, maintain and implement procedures to protect the security and confidentiality of requests from anyone with regard to the protection of customers' nonpublic information.

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. 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 financing 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.

3. Checking the list of wanted criminals and the list of economic sanctions and embargoes

Before opening a new account, our AML Compliance Officer will check to ensure that the client is not on the list of wanted criminals or is not engaged in transactions prohibited by economic sanctions and embargoes administered and enforced by the country in which we do business. As the list of wanted criminals and the list of economic sanctions and embargoes (hereinafter referred to as the List) are updated regularly, we will refer to them periodically and subscribe to receive any updates. As for the List, we may also access it through various software programs to ensure speed and accuracy. Our AML Compliance Officer will also review existing accounts against the List as they are updated and he will document the review.

If we determine that a customer is on a list or is engaging in transactions prohibited by economic sanctions and embargoes administered and enforced by the country in which we do business, we will refuse the transaction and/or freeze the client's assets and send the information about blocked assets and/or the refused transaction to the requestor within 10 days. We will also call the Hotline if necessary.

Our review will include customer accounts, customer-related transactions (including company-passing activity such as wire transfers) and assessment of related customer transactions to physical security certificates or application-based investments.

4. Customer Identification Program

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 and compare customer identification information with

government-provided lists of suspected terrorists, once such lists have been issued by the government.

We do not open or maintain customer accounts, in that we do not establish formal relationships with “customers” for the purpose of effecting transactions in crypto. If in the future the firm elects to open customer accounts or to establish formal relationships with customers for the purpose of effecting transactions in crypto, we will first establish, document and ensure the implementation of appropriate procedures.

a. Required Customer Information

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

- (1) the name;
- (2) date of birth (for an individual);
- (3) an address, which will be a residential or business street address (for an individual), or the residential or business street address of a 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, or one or more of the following: a taxpayer identification number (for legal entity), passport number and country of issuance, foreigner 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.

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.

b. Customers Who Refuse to Provide Information

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

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. Our team will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).

We will verify customer identity through documentary means, non-documentary means or both. We will use documents to verify customer identity when appropriate documents are available. 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. In verifying the information, we will consider whether the identifying information that we receive, such

as the customer's name, street address, zip code, telephone number (if provided), date of birth and Social Security number, allow us to determine that we have a reasonable belief that we know the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).

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

- For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguards, 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 sources.
- Checking references with other financial institutions; or
- Obtaining a financial statement.

We will use non-documentary methods of verification when:

- (1) the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;
- (2) the firm is unfamiliar with the documents the customer presents for identification verification;
- (3) the customer and firm do not have face-to-face contact; and
- (4) other circumstances increase the risk that the firm will be unable to verify the true identity of the customer through documentary means.

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

We recognize that the risk that we may not know the customer's true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated as a primary money laundering jurisdiction, a terrorist concern, or has been designated as a non-cooperative country or territory. We will identify customers that pose a heightened risk of not being properly identified. We will also take additional measures that may be used to obtain information about the identity of the individuals associated with the customer when standard documentary methods prove to be insufficient (such as obtaining information about beneficial ownership, individuals with authority or control over such account)

d. Lack of Verification

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

e. Recordkeeping

We will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. We will also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We will retain records of all identification information for five years after the account has been closed; we will retain records made about verification of the customer's identity for five years after the record is made.

f. Comparison with Government-Provided Lists of Terrorists

At such time as we receive notice that a government agency has issued a list of known or suspected terrorists and identified the list as a list for government purposes, we will, within a reasonable period of time after an account is opened), determine whether a customer appears on any such list of known or suspected terrorists or terrorist organizations issued by any government agency. We will follow all government directives issued in connection with such lists.

g. Notice to Customers

We will provide notification to customers that the firm is requesting information from them to verify their identities, as required by government law. We will use the following method to provide notice to customers: telephone, online, email, text message... etc.

Important Information About Procedures for Opening a New Account:

To help the government fight the funding of terrorism and money laundering activities, government law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account.

What this means for you: When you open an account, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

h. Reliance on Another Financial Institution for Identity Verification

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 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, and is regulated by a government 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.

5. Customer Due Diligence Rule

In addition to the information collected under the written Customer Identification Program, 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. 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.

We do not open or maintain accounts for legal entity customers. If in the future the firm elects to open accounts for legal entity customers, we will first establish, document and ensure the implementation of appropriate CDD procedures.

a. Identification and Verification of Beneficial Owners

At the time of opening an account for a legal entity customer, our AML Compliance Officer 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 residential or business street address of a 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 one or more of the following: a passport number and country of issuance, or other similar identification numbers, such as an 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 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.

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 our methods .

Depending on the facts and circumstances, a customer risk profile may include such information as:

- 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.

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).

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

We will review our accounts to determine whether we offer any private banking accounts and we will conduct due diligence on such accounts. This due diligence will include, at least: (1) ascertaining the identity of all nominal holders and holders of any beneficial ownership interest in the account (including information on those holders' lines of business and sources of wealth); (2) ascertaining the source of funds deposited into the account; (3) ascertaining whether any such holder may be a senior foreign political figure; and (4) detecting and reporting, in accordance with applicable laws and regulations, any known or suspected money laundering, or use of the proceeds of foreign corruption.

We will review public information, including information available in Internet databases, to determine whether any private banking account holders are senior foreign political figures. If we discover information indicating that a particular private banking account holder may be a senior foreign political figure, and upon taking additional reasonable steps to confirm this information, we determine that the individual is, in fact, a

senior foreign political figure, we will conduct additional enhanced due diligence to detect and report transactions that may involve money laundering or the proceeds of foreign corruption.

In so doing, we will consider the risks that the funds in the account may be the proceeds of foreign corruption by determining the purpose and use of the private banking account, location of the account holder(s), source of funds in the account, type of transactions conducted through the account and jurisdictions involved in such transactions. The degree of scrutiny we will apply will depend on various risk factors, including, but not limited to, whether the jurisdiction the senior foreign political figure is from is one in which current or former political figures have been implicated in corruption and the length of time that a former political figure was in office. Our enhanced due diligence might include, depending on the risk factors, probing the account holder's employment history, scrutinizing the account holder's source(s) of funds, and monitoring transactions to the extent necessary to detect and report proceeds of foreign corruption, and reviewing monies coming from the government, government-controlled or government enterprise accounts (beyond salary amounts).

If we do not find information indicating that a private banking account holder is a senior foreign political figure, and the account holder states that he or she is not a senior foreign political figure, then we may make an assessment if a higher risk for money laundering, nevertheless, exists independent of the classification.

In either case, if due diligence (or the required enhanced due diligence, if the account holder is a senior foreign political figure) cannot be performed adequately, we will, after consultation with the firm's AML Compliance Officer and, as appropriate, not open the account, suspend the transaction activity, report to government, close the account and/or take other appropriate action.

7. Compliance with the Government 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 the Government 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 Government's final rule and follow any prescriptions or prohibitions contained in that rule.

For example, if the final rule deems a certain bank and its subsidiaries (Specified Banks) to be of primary money laundering concern, a special measure may be a prohibition from opening or maintaining a correspondent account, or on behalf of, the Specified Banks. In that case, we will take the following steps:

- (1) We will review our account records, including correspondent account records, to ensure that our account holders and correspondent account holders maintain no accounts directly for, or on behalf of, the Specified Banks; and
- (2) We will apply due diligence procedures to our correspondent accounts that are reasonably designed to guard against the indirect use of those accounts by the Specified Banks. Such due diligence may include:

- Notification to Correspondent Account Holders

We will notify our correspondent account holders that the account may not be used to provide the Specified Banks with access to us.

We will transmit the notice to our correspondent accounts using our method, and we shall retain documentation of such notice.

- Identification of Indirect Use

We will take reasonable steps in order to identify any indirect use of our correspondent accounts by the Specified Banks. We will determine if such indirect use is occurring from transactional records that we maintain in the normal course of business. We will take a risk-based approach when deciding what, if any, additional due diligence measures we should adopt to guard against the indirect use of correspondent accounts by the Specified Banks, based on risk factors such as the type of services offered by, and geographic locations of, their correspondents.

We understand that we have an ongoing obligation to take reasonable steps to identify all correspondent account services our correspondent account holders may directly or indirectly provide to the Specified Banks.

8. Monitoring Accounts for Suspicious Activity

We will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business. (Red flags are identified in Section 10.b. below.) Monitoring will be conducted through our methods. The customer risk profile will serve as a baseline for assessing potentially suspicious activity. The AML Compliance Officer 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.

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 hotline.

b. Red Flags

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

(1) 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 openings.
- 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 that 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 purposes.
- An account is opened by a politically exposed person (PEP), particularly in conjunction with one or more additional risk factors, such as the account being opened by a shell company beneficially owned or controlled by the PEP, the PEP is from a country which has been identified by Government 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.
- 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.
- 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.

(2) 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 evading 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 orders (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.

- 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
- 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 crypto account is used for payments or outgoing wire transfers with little or no securities activities (i.e., the 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.
- 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).
- 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.

(3) Other Potential Red Flags

- The customer is reluctant to provide the 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.
- 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 the normal activities of the customer.
- 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 unusual financial activity.

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 our AML Compliance Officer. Under the direction of the AML Compliance Officer, 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 reporting to the government.

9. Suspicious Transactions and Reporting

a. Reporting

We will file a report with the Government for any transactions (including deposits and transfers) conducted or attempted by, at or through our firm involving \$10,000 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 government law or regulation or to avoid any transaction reporting requirement under government law or regulation;
- (2) the transaction is designed, whether through structuring or otherwise, to evade any requirements of the law;
- (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, the 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. 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 law. 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

the Government, any other appropriate law enforcement agencies, government 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 law. 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 Government, or another appropriate law enforcement or regulatory agency, decline to produce the SAR or to provide any information that would disclose that a SAR was prepared or filed. We will notify the Government of any such request and our response.

b. 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 country we had a business, 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 report to these governments if we discover that we have received or caused or attempted to receive from outside of these 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 report 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).

10. AML Recordkeeping

a. Responsibility for Required AML Records and reporting.

Our AML Compliance Officer 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 law and other recordkeeping requirements.

b. SAR Maintenance and Confidentiality

We will hold SARs and any supporting documentation confidential. We will not inform anyone outside of the Government or other appropriate law enforcement or regulatory agencies about 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 the Government of any such subpoena requests that we receive. We will segregate SAR filings and copies of supporting documentation from other firms' books and records to avoid disclosing SAR filings. Our AML Compliance Officer 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. 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.

c. Additional Records

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

- Each document granting a signature or trading authority over each customer's account;
- 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 country we had business; and
- A record of each receipt of currency, other monetary instruments 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 country we had business.

11. 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 AML regulations. 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 the Government website. As a general matter, we will obtain and use the following exception reports offered by our clearing firm in order to monitor customers 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 law and its implementing regulations.

12. Training Programs

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

Our training will include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, the filing of SARs); (3) what employees' roles are in the firm's compliance efforts and how to perform them; (4) the firm's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the law.

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 based on the Certified Anti-Money Laundering Specialist program by ACAMS organization. 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.

13. 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 Officer. We will also review the AML performance of supervisors, as part of their annual performance review. The AML Compliance Officer's accounts will be reviewed by our senior accountant.

14. Confidential Reporting of AML Non-Compliance

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

15. 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 the signatures below.

16. AML Compliance Officer Designation and Duties

The duties of the AML Compliance Officer will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees. The AML Compliance Officer 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 Government when appropriate. The AML Compliance Officer is vested with full responsibility and authority to enforce the firm's AML program.

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

THE END