HOLISTIC BROKERAGE

# Anti-Money Laundering Program

# Policies and Procedures

## May 2022

# Table of Contents

## I. Firm Program

It is the Program of Holistic Brokerage LLC. ("Holistic" or 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[1] ("BSA") and its implementing regulations. Money laundering is generally defined as engaged in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. The process generally involves three stages:

1. Placement – the placement of illicit funds into the financial system by converting those funds into some other financial instrument or medium;

2. Layering – illicit funds are moved to other accounts or other financial institutions to obscure the origins of the funds; and

3. Integration – illicit funds are used to acquire legitimate assets or fund further criminal or legitimate activities.

This anti-money laundering ("AML") program and the internal controls of the Firm are designed to ensure compliance with all applicable BSA regulations and Financial Industry Regulatory Authority ("FINRA") rules and will be reviewed and updated on a regular basis to ensure appropriate procedures and internal controls are in place to account for changes in regulations and changes in our business.

As a general matter, the AML laws and regulations in the United States:

- make it a criminal offense to knowingly, or with willful blindness, engage in financial transactions or to transmit overseas funds that represent the proceeds from an extensive list of specified crimes; and

- require financial institutions to identify and report certain customer transactions and suspicious customer activity and to create documentation that will allow law enforcement authorities to trace illicit funds back to their illegal origins.

Section 352 of the USA PATRIOT Act of 2001,[2] signed into law on October 26, 2001, amended the BSA to require, among other things, that financial institutions[3] establish AML

---

[1] 31 U.S.C. § 5311 et seq.

[2] *Uniting And Strengthening America by providing Appropriate Tools to Intercept and Obstruct Terrorism Act of 2001,* Public Law No. 107-56, 115 Stat. 272 (2001).

[3] The term "financial institution" is defined in Section 5312(a)(2) of the BSA to include securities broker dealers like the Firm.

programs. In addition, on April 22, 2002, the U.S. Securities and Exchange Commission (the "SEC") approved a rule by FINRA -- Rule 3310 (formerly NASD Rule 3011) -- which requires that member firms develop AML programs designed to achieve and monitor compliance with the BSA and related regulations. Member firms are obligated, at a minimum, to:

- Develop internal policies, procedures and controls to guard against money laundering, including but not limited to achieving compliance with the applicable provisions of the BSA and the implementing regulations hereunder;
- Designate a compliance officer responsible for implementing and monitoring those internal policies, procedures and controls;
- Provide ongoing employee training with respect to those internal policies, procedures and controls; and
- Provide for an independent testing function to check compliance of the AML programs.

Holistic is a broker-dealer registered with FINRA. Holistic serves as the introducing broker on a fully disclosed basis, for clients in connection with purchases and sales of various types of securities for institutional and retail (high net worth) customers. Generally, Holistic does not directly handle the assets (e.g., securities, cash, etc.) of its customers. The purchase or sale of securities for Holistic's clients will generally be provided through a third party, such as a clearing broker. Clients introduced by Holistic will generally be required to deliver cash or securities to and receive cash or securities from the clearing broker.

Holistic does not offer or sell proprietary products or research. Holistic does not engage in underwriting or market making activity. Holistic does not maintain client assets, securities or maintain discretionary authority over customer accounts.

Holistic will use a third-party clearing broker to provide services to its various customers, including the processing of shareholder applications and purchase, redemption and exchange orders. Employees of Holistic may not receive shareholder assets (e.g., securities, cash, etc.) directly. All such assets shall be directed to a third-party clearing broker. Each such third-party clearing broker shall have instituted an AML program that complies with the standards required by the BSA. Holistic shall obtain a copy of such clearing broker's AML program. When Holistic is acting as an introducing broker, employees of Holistic shall verify the identity of the customer. Holistic shall cooperate fully with its clearing brokers in monitoring customers for potential suspicious activities that may indicate money-laundering activities.

## II. AML Compliance Officer Designations and Duties

Holistic designates Gustavo Dominguez as the Firm's AML Compliance Officer ("AML Compliance Officer", "AMLCO") who will be responsible for oversight of this AML Program. Mr. Dominguez also serves as the Firm's Chief Compliance Officer ("CCO"). The AML

Compliance Officer is vested with full responsibility and authority to enforce the Firm's AML Program.

The AML Compliance Officer shall hold a meeting with all of Holistic's officers and employees at least once each year to train them with respect to this Program (including modifications to this Program required by applicable law, rule or regulation), provide updated information regarding Holistic's AML practices and answer questions regarding Holistic's AML practices. The AML Compliance Officer shall monitor industry developments with respect to AML practices, rules or regulations, and suggest appropriate changes or modifications to this AML Program. 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 (SAR-SFs) are filed with the Financial Crimes Enforcement Network ("FinCEN") when appropriate.

The Firm will also disclose to FINRA via the FINRA Contact System ("FCS") on FINRA's web site the name, title, mailing address, e-mail address, telephone number, and facsimile number of the AML Compliance Officer. Any changes to the contact information of the AML Compliance Officer (or if such officer changes) will be promptly updated on the FCS. Pursuant to NASD Rule 1160, a review, and if necessary, an update of the FCS will be conducted within 17 business days after the end of each calendar year. The annual review of FCS information will be conducted by CCO 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, CCO will update the information promptly, but in any event not later than 30 days following the change.

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

### *A.* FinCEN Requests Under PATRIOT Act Section 314(a)

Holistic will respond to a FinCEN request (a "314(a) Request") about accounts or 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 a 314(a) Request as outlined in the Frequently Asked Questions (FAQ) located on FinCEN's secure Web site. We understand that we have 14 days (unless otherwise specified by FinCEN) from the transmission date of the request to respond to a 314(a) Request. We will designate through the 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. All 314(a) Requests are sent to the AML Compliance Officer via email. The AML Compliance Officer shall search and compare our customer data base to the 314(a) Request. The AMLCO will evidence in writing the review date the review was conducted, the FinCEN response due date, and whether or not a match was found.

Unless otherwise stated in the 314(a) Request, we are required to search current accounts, accounts maintained by a named suspect during the preceding 12 months, and transactions conducted by or on behalf of or with a named subject during the preceding six months. If we

find a match, we will promptly respond through FinCENs' secure information system. If the search parameters differ from those mentioned above (for example, if FinCEN requests longer periods of time or limits the search to a geographic location), we will limit our search accordingly.

If we search our records and do not uncover a matching account or transaction, then we will not reply to 314(a) Request. Upon completion of the FinCEN list comparison to the Firm's customer account database the Firm completes the "self-verification" via FinCEN's website. The self-verification documentation is maintained by the Firm to evidence its timely review.

We will not disclose to anyone (including our customer in question) the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. We will review, maintain and implement procedures to protect the security and confidentiality of requests from FinCEN similar to those established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act of 1999 with regard to the protection of customers' non-public personal information.

We will direct any questions we have about the 314(a) Request to the requesting federal law enforcement agency as designated in the 314(a) Request.

Unless otherwise stated in the 314(a) Request, we will not be required to treat the Request as continuing in nature, and we will not be required to treat the Request as a list for purposes of the customer identification and verification requirements. We will not use information provided to FinCEN for any purpose other than: (1) to report to FinCEN as required under Section 314 of the PATRIOT Act; (2) to determine whether to establish or maintain an account, or to engage in a transaction; or (3) to assist the Firm in complying with any requirement of Section 314 of the PATRIOT Act.

### *B. National Security Letters*

National Security Letters ("NSLs") are written investigative demands that may be issued by the local Federal Bureau of Investigation and other federal government authorities conducting counterintelligence and counterterrorism investigations to obtain, among other things, financial records of broker-dealers. NSLs are highly confidential. No broker-dealer, officer, employee or agent of the broker-dealer can disclose to any person that a government authority or the FBI has sought or obtained access to records. If the Firm files a Suspicious Activity Report (SAR-SF) after receiving a NSL, the SAR-SF should not contain any reference to the receipt or existence of the NSL.

### *C. 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-SF). When the Firm receives a grand jury subpoena, it will conduct a risk assessment of the customer subject to the subpoena as well as review the customer's account activity. If the Firm uncovers suspicious activity during our risk assessment and review, we will elevate that customer's risk assessment

and file a SAR-SF in accordance with the SAR-SF filing requirements. The Firm understands that none of its 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 Holistic used to respond to it. To maintain the confidentiality of any grand jury subpoena we receive, the Firm will process and maintain the subpoena by only permitting the AML Compliance Officer to review and maintain a copy of such subpoena, provided that the AML Compliance Officer may furnish a copy of such subpoena to the legal counsel of the Firm. If the Firm files a SAR-SF after receiving a grand jury subpoena, the SAR-SF will not contain any reference to the receipt or existence of the subpoena. The SAR-SF will only contain detailed information about the facts and circumstances of the detected suspicious activity.

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

We may in our sole discretion 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. If the Firm decides to share such information, the AML Compliance Officer will ensure that the Firm files with FinCEN an initial notice before any sharing occurs and annual notices thereafter. The Firm will use the notice form found at www.fincen.gov. Before the Firm 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. This requirement applies even to financial institutions *with which we are affiliated*, and that the Firm 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.

### *E. Joint Filing of SARs by Broker-Dealers and Other Financial Institutions*

The Firm in its discretion may file a joint SAR. 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-SF.

We will share information about particular suspicious transactions with our clearing broker RBC Correspondent Services or Pershing, LLC (as applicable), for purposes of determining whether we and our clearing broker will file jointly a SAR-SF. In cases in which we file a joint SAR-SF 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-SF.

If we determine it is appropriate to jointly file a SAR-SF, we understand that we cannot disclose that we have filed a SAR-SF 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-SF concerns the other broker-dealer or one of its employees), we understand that we cannot disclose that we have filed a SAR-SF to any other financial institution or insurance Firm.

## IV. Checking the Office of Foreign Assets Control ("OFAC") List

As a part of its due diligence when entering into a client relationship, Holistic will conduct a database search using the OFAC/FINRA website (ofac.finra.org) or similar third-party vendor. This service will help us to comply with OFAC, PATRIOT Act and our Customer Identification Program (discussed in Section V below).

Before opening an account, and on an ongoing basis, we will check to ensure that a customer does not appear on Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" List ("SDN List") and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC Web Site. We will also review existing accounts against these lists when they are updated and we will document our review. Other financial transactions must be reviewed for OFAC compliance, including deposits, wire and ACH transfers, withdrawals, and exchanges. In addition, the names of all parties to a transaction must be checked against the list of names of individuals, entities, geographical locations or countries that have been identified by OFAC. This includes, but is not limited to, beneficiaries, owners, and receiving and sending parties. The Firm continuously verifies and reviews its customer account database for possible OFAC matches. The Firm's AML Compliance Officer or designee is responsible for reviewing and assessing information provided for further required action.

In the event that we determine a customer, or someone with or for whom the customer is transacting, is on the SDN List or is from or engaging in transactions with a person or entity located in an embargoed country or region, we will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC. We will also call the OFAC Hotline at 1-800-540-6322. Reports filed by the Firm will be retained in a file for a period of at least five years for blocked accounts or securities. Information to be reported includes:

For rejected disbursements, the following information is to be filed:

- Name and address of the transferee financial institution
- Date and amount of the transfer
- Copy of the payment or transfer instructions
- Basis for rejection
- Name and phone number of contact person at the Firm

On an annual basis by September 30, the clearing firm, or where appropriate the Firm, will file Form TDF 90-22.50 with OFAC for any blocked property held as of June 30.

The AML Compliance Officer shall respond to any formal request made by federal law enforcement authorities concerning any client accounts no later than seven (7) days after the receipt of such request. The AML Compliance Officer shall provide such information such as: (i) information concerning the client's identity; (ii) the account number; (iii) any identifying information provided by the account holder; and (iv) information concerning account activity. Holistic shall work with any third-party clearing brokers to ensure their cooperation. All such information shall be provided, as possible, in the format specified in the formal request.

## V. Monitoring Employee Conduct and Accounts

### *A. CIP – Background*

As part of the Firm's Customer Identification Program ("CIP") adopted pursuant to Section 326 of the USA PATRIOT Act and the BSA, the AML Compliance Officer will instruct associates to verify the identity of customers to the extent reasonable and practical as part of its AML Program.

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

For purposes of the CIP, a "customer" is defined as a person who opens a new account (the "accountholder"). An "account" is defined as a formal relationship with the Firm established to effect transactions in securities, including, but not limited to, the purchase or sale of securities. Exclusions from the definition of customer include certain transferred accounts (any account acquired through an acquisition, merger, purchase of assets, or assumption of liabilities, including transfers of accounts that result from the Firm changing its clearing firm) and accounts opened for the purpose of participating in an employee benefit plan established pursuant to ERISA. Although the Firm is not required to verify the identity of a customer whose

account is transferred to the Firm (and the clearing firm) if the customer does not initiate the transfer, the Firm will consider the risks of a particular transferred account to determine if an associate must obtain and verify information from the transferred customer.

Also excluded from the definition of customer are financial institutions regulated by a federal functional regulator, banks regulated by a state bank regulator, governmental agencies, and publicly traded companies.[3] Persons who have authority over accounts, fill out account opening paperwork, or provide information necessary to open the account are not considered customers, if such persons are not accountholders as well. Minors and non-legal entities are not considered customers; in these cases, the person who fills out the account-opening paperwork and provides the information necessary to open the account in the name of the minor or non-legal entity is considered the customer.

### *B. Information Collected At Inception*

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

(1) the name;

(2) date of birth (for an individual);

(3) an address, which will be a residential or business street address (for an individual), an Army Post Office (APO) or Fleet Post Office (FPO) box number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address), or a principal place of business, local office, or other physical location (for a person other than an individual); and

(4) an identification number, which will be a taxpayer identification number (for U.S. persons), or one or more of the following: a taxpayer identification number, passport number and country of issuance, alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard (for non-U.S. persons).

In the event that a customer has applied for, but has not received, a taxpayer identification number, we will consult with our legal counsel to confirm that the application was filed before the customer opens the account and to obtain the taxpayer identification number within a reasonable period of time after the account is opened.

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

[3] Only to the extent of domestic operations; foreign offices, affiliates, or subsidiaries of publicly traded companies are not exempt from CIP requirements.

### *C. 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, the AML Compliance Officer will be notified so that we can determine whether we should report the situation to FinCEN on a SAR-SF.

### *D. Verifying Information*

Based on the risk, and to the extent reasonable and practicable, Holistic will ensure that we have a reasonable belief that we know the true identity of our customers by using various sources including, but not limited to internet, third party vendor searches to verify and document the accuracy of the information we receive about our customers. CCO 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 evidence, non-documentary evidence, 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 non-documentary means described below whenever necessary. We may also use such non-documentary means, after using documentary evidence, 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).

#### 1. *Documentary Methods to Verify Identity*

Appropriate documents for verifying the identity of customers include, but are not limited to, the following:

- For an individual, an unexpired government-issued identification evidencing nationality, 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.

Holistic understands that it is 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.

2. *Non-Documentary Methods to Verify Identity*

Holistic will use the following non-documentary methods of verifying identity, such as:

a. contacting a customer;

b. independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from LexisNexis, a public database, or other similar non-documentary source;[4]

c. checking references with other financial institutions; or

d. obtaining a financial statement.

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

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

b. when the Firm is unfamiliar with the documents the customer presents for identification verification;

c. when the customer and Firm do not have face-to-face contact; and

d. when there are other circumstances that increase the risk that the Firm will be unable to verify the true identity of the customer through documentary means.

We will verify the information within a reasonable time before or after the account is opened.[5] 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 SAR-SF in accordance with applicable laws and regulations.

[4] LexisNexis® Risk Solutions and its sister company LexisNexis® Legal & Professional are part of RELX Group, a global provider of information and analytics for professional and business customers across industries. The group serves customers in more than 180 countries and has offices in about 40 countries. It employs approximately 30,000 people of whom half are in North America. LexisNexis® Risk Solutions provides customers with solutions and decision tools that combine public and industry specific content with advanced technology and analytics to assist them in evaluating and predicting risk and enhancing operational efficiency.

[5] The Firm defines "reasonable" as one (1) week. This serves as a general guideline and best practice.

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

In addition, we will verify the identity of certain customers, such as obtaining information about individuals with authority or control over such account by using the above-mentioned documentary procedures and, if necessary, non-documentary procedures.

### *E. Lack of Verification*

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

### *F. Recordkeeping*

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

### *G. Comparison with Government-Provided Lists of Terrorists and Criminals*

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 with OFAC rules prohibiting transactions with certain foreign countries or their nationals.

### *H. Notice to Customers*

We will provide notice to customers that the firm is requesting information from them to verify their identities, as required by Federal law. We will provide notice to customers by telephone or in person and as part of their account-opening documentation, and the notice shall be as follows:

> **Important Information About Procedures for Opening a New Account**
>
> To help the government fight the funding of terrorism and money laundering activities, United States 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 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.

The Firm may also include a notice on its website relating to its customer identification obligations and account opening documentation requirements.

## VI. General and Enhanced Customer Due Diligence

It is important to our AML and SAR-SF reporting program that we obtain sufficient information about each customer to allow us to evaluate the risk presented by that customer and to detect and report suspicious activity. When we open an account for a customer, the due diligence we perform may be in addition to customer information obtained for purposes of our CIP. The Firm and its registered representatives must be particularly mindful when establishing accounts domiciled in "high risk" regions, as wells accounts for "Clients who are neither Widely Known nor Known to the Broker-dealer.

Specifically, registered representatives should be mindful of the issues discussed below when obtaining information with respect to the following persons or entities that are not widely Known or Known to Broker-Dealer:

- **Natural Persons.** In addition to New Account Documentation, registered representatives should obtain information about the source of the individual's net worth -- particularly where a substantial portion comes from sources other than an employer and the individual is unknown to the Firm.

- **Non-Resident Aliens.** Registered representatives should obtain a current passport number or other valid government identification number and obtain all necessary U.S. tax forms. Registered representatives should notify the AML Compliance Officer if the NRA is from a country that is or has been involved in suspected terrorist activities.

- **Legal Entities.** Includes a corporation, limited liability company, or other entity that is created by a filing of a public document with a Secretary of State or similar office, a general partnership, and any similar business entity formed in the United States or a foreign country. **Legal entity** does not include sole proprietorships, unincorporated associations, or natural persons opening accounts on their own behalf. Registered representatives are required to obtain a "Certification Regarding Beneficial Owners of Legal Entity Customers" pursuant to Federal Regulation Title 31 CFR Section 1010.230 – Beneficial ownership requirements for legal entity customers.

- **Foreign Operating Commercial Entities.** Registered representatives should obtain the appropriate organizational documents. If the registered representative has any questions about the authenticity of the documents or risks posed by the country of organization, he or she should contact the Firm's AML Compliance Officer.

- **Offshore Trusts.** Registered representatives should identify the sponsors and beneficiaries of any trust and consult with the AML Compliance Officer as to whether further due diligence is required for trusts established in jurisdictions that lack regulatory oversight over trust formation.

- **Institutional Accounts, Hedge Funds, Investment Funds, and Other Intermediary Relationships.** Registered representatives are required to comply with Broker-Dealer's procedures relating to transactions with institutional clients and consult the AML Compliance Officer as to whether further due diligence is required for an institutional client that presents potential risk.

- **FATF Watch List Countries and/or Countries with Weak AML Regimes.** Accounts domiciled in such locations pose elevated and/or significant AML based risks due to the higher probability that funds may be derived from illegal and/or corrupt sources.

The above list is not exhaustive and if registered representatives have problems obtaining information adequate to validate a client's identity, they should consult with the AML Compliance Officer to determine whether additional forms of identification should be obtained.

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

(1) ascertaining and obtaining adequate documentation regarding 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 or a close relative thereof;

(4) detecting and reporting, in accordance with applicable law and regulation, any known or suspected money laundering and/or use of the proceeds of foreign corruption;

(5) establishing the account objectives and anticipated account activity;

(6) reviewing the necessary documents for any corporate entity that may exist and the purpose for its existence and for the opening of the account;

(7) personally meet the client;

(8) perform an OFAC search to conclude that the client is not a specially-designated national;

(9) perform background searches on the beneficial owner with public information sources; and

(10) require the Holistic relationship manager to document how long he or she has known the customer and under what circumstances he or she came to meet the customer via memorandum and/or the Firm's Enhanced Due Diligence Questionnaire "EDD" questionnaire form.

## VII. Foreign Correspondent Accounts and Foreign Shell Banks

Holistic will detect correspondent accounts (any account that permits a foreign bank to engage in securities or futures transactions, funds transfers, or other types of financial transactions) for unregulated foreign shell banks by requiring that all new accounts opened by the firm be reviewed by the Compliance Officer who shall determine whether the customer is a foreign bank. Upon finding or suspecting such accounts, firm employees will notify the AML Compliance Officer, who will terminate any verified correspondent account in the United States for an unregulated foreign shell bank. We will also terminate any correspondent account that we have determined is not maintained by an unregulated foreign shell bank but is being used to provide services to such a shell bank. We will exercise caution regarding liquidating positions in such accounts and take reasonable steps to ensure that no new positions are established in these accounts during the termination period. We will 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.

### *A. Certifications*

Holistic will require our foreign bank account holders to complete a certification in the form attached hereto. We will send the certification forms to our foreign bank account holders for completion, which requires them to certify that they are not shell banks and to provide ownership and agent information. We will re-certify when we believe that the information is no longer accurate and at least once every three years. We will start the re-certification process at least 90 days before the current certification expires to allow enough time to process.

The Firm uses an internal Foreign Bank Certification spreadsheet to monitor and track certifications to all of its foreign bank account holders. On a monthly basis, Holistic compares a Pershing monthly exception report to the Foreign Bank Certification spreadsheet, which will be updated as necessary.

### *B. Recordkeeping for Foreign Correspondent Accounts*

We will keep records identifying the owners of foreign banks with U.S. correspondent accounts and the name and address of the U.S. agent for service of legal process for those banks.

### *C. Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationships*

When we receive a written request from a federal law enforcement officer for information concerning correspondent accounts, we will provide that information to the requesting officer not later than 7 days after receipt of the request. We will close, within 10 days, any account for a bank that we learn from Treasury or the Department of Justice has failed to comply with a summons or has contested a summons, and we will exercise our discretion to close any account based on the information requested. We will scrutinize any account activity during that 10-day period to ensure that any suspicious activity is appropriately reported and to ensure that no new positions are established in these accounts.

## VIII. Entities or Jurisdictions Designated as "Primary Money Laundering Concern"

Section 311 of the Patriot Act amended the BSA and provided the U.S. Secretary of the Treasury with the authority to require financial institutions to take certain "special measures" against a jurisdiction, institution, class of transaction, or type of account that is of 'primary money laundering concern.' Section 311 gives the government the tools to put additional pressure on those jurisdictions and institutions that pose significant money laundering threats. Section 311 provided for five different special measures that can be imposed, either individually, jointly, or in any combination:

1. Additional recording and reporting of certain financial institutions;

2. Information relating to beneficial ownership;

3. Information relating to certain payable through accounts;

4. Information relating to certain correspondent accounts; and

5. Prohibitions or conditions on opening or maintaining certain correspondent or payable through accounts.

*Client Database Review*. Holistic will receive and maintain a file containing all notifications received from FinCEN identifying special measure jurisdictions, financial institutions, or international transactions of primary money laundering concerns. Upon notification from FinCEN about the addition of a "special measure" institution / jurisdiction, the Firm's entire current and prospective client list will be reviewed to identify all "special measure" financial institutions/jurisdictions. If information indicating that the "special measure" financial institution/jurisdiction is not a client or prospect of the Firm then additional enhanced due diligence will not be required. If, however, information is discovered indicating that a particular institution/jurisdiction is possibly subject to special measures, enhanced due diligence will be conducted to detect and report transactions that are required pursuant to the "special measure" issued."

*Special Measures Notices*. In addition, under the special measures, all financial institutions and broker-dealers are subject to the following two primary requirements with respect to non-U.S. banks and other non-U.S. financial institutions (the "Specified Banks") subject to special measures:

- The prohibition from opening or maintaining a correspondent account in the United States for or on behalf of, the Specified Banks, and
- Due Diligence upon correspondent accounts to prohibit indirect use.

The Firm will send written notification to all correspondent account holders that the account may not be used to provide the Specified Banks with access to the Firm. The written notification will be provided to correspondent accounts at the time the accounts are opened and mailed annually or within 30 days following an update to the Section 311 – Special Measures list, whichever is sooner.

The AML Compliance Officer or designee is responsible for monitoring the Section 311 list, which can be found at https://www.fincen.gov/resources/statutes-and-regulations/311-special-measures, for updates.

The Firm's notification letter must be sent to all non-U.S. correspondent account customers and contain the following statement:

> "*Notice*: Pursuant to U.S. regulations issued under section 311 of the USA PATRIOT Act, 31 CFR 103.192, we are prohibited from opening or maintaining a correspondent account for, or on behalf of, [the Specified Banks]. The regulations also require us to notify you that your correspondent account with our financial institution may not be used to provide [the Specified Banks] with access to our financial institution. If we become aware that [the Specified Banks] are indirectly using the correspondent account you hold at

our financial institution, we will be required to take appropriate steps to prevent such access, including terminating your account."

The Firm will keep a log to evidence the delivery of the notice and will be kept on file for 3 years. The new accounts department will be responsible for sending the notice to both existing and new accounts for foreign correspondent accounts.

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

### *A. Requirements*

We will conduct an inquiry to determine whether a foreign financial institution has a correspondent account established, maintained, administered or managed by the firm.

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

The relevant risk factors can include:

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

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

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

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

### *B. Enhanced Due Diligence*

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

(1) an offshore banking license;

(2) a banking license issued by a foreign country that has been designated as non-cooperative with international anti-money laundering principles or procedures by an intergovernmental group or organization of which the United States is a member and with which designation the U.S. representative to the group or organization concurs; or

(3) a banking license issued by a foreign country that has been designated by the Secretary of the Treasury as warranting special measures due to money laundering concerns.

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

(1) conduct enhanced scrutiny of the correspondent account to guard against money laundering and to identify and report any suspicious transactions. Such scrutiny will not only reflect the risk assessment that is described in Section 8.a. above, but will also include procedures to, as appropriate:

(i) obtain (*e.g.,* using a questionnaire) and consider information related to the foreign bank's AML program to assess the extent to which the foreign bank's correspondent account may expose us to any risk of money laundering;

(ii) monitor transactions to, from or through the correspondent account in a manner reasonably designed to detect money laundering and suspicious activity (this monitoring may be conducted manually or electronically and may be done on an individual account basis or by product activity); and

(iii) obtain information from the foreign bank about the identity of any person with authority to direct transactions through any correspondent account that is a payable-through account (a correspondent account maintained for a foreign bank through which the foreign bank permits its customer to

engage, either directly or through a subaccount, in banking activities) and the sources and beneficial owners of funds or other assets in the payable-through account.

(2) determine whether the foreign bank maintains correspondent accounts for other foreign banks that enable those other foreign banks to gain access to the correspondent account under review and, if so, to take reasonable steps to obtain information to assess and mitigate the money laundering risks associated with such accounts, including, as appropriate, the identity of those other foreign banks; and

(3) if the foreign bank's shares are not publicly traded, determine the identity of each owner and the nature and extent of each owner's ownership interest. We understand that for purposes of determining a private foreign bank's ownership, an "owner" is any person who directly or indirectly owns controls or has the power to vote 10 percent or more of any class of securities of a foreign bank. We also understand that members of the same family shall be considered to be one person.

### *C. Special Procedures When Due Diligence or Enhanced Due Diligence Cannot Be Performed*

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

## X. 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. A "private banking" account is an account (or any combination of accounts) maintained by Holistic that: (i) requires a minimum aggregate amount of at least $1 million in assets; (ii) is established on behalf of or for the benefit of one or more non-U.S. persons; and (iii) is assigned to, or is administered or managed by, an officer, employee or agent of Holistic acting as a liaison between the Firm and the direct or beneficial owner of the account. See 31 C.F.R. § 103.175(o).

This due diligence will include, at least:

(1) ascertaining and obtaining adequate documentation regarding 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 or a close relative thereof;

(4) detecting and reporting, in accordance with applicable law and regulation, any known or suspected money laundering and/or use of the proceeds of foreign corruption;

(5) establishing the account objectives and anticipated account activity;

(6) reviewing the necessary documents for any corporate entity that may exist and the purpose for its existence and for the opening of the account;

(7) personally meet the client;

(8) perform an OFAC search to conclude that the client is not a specially-designated national;

(9) perform background searches on the beneficial owner with public information sources; and

(10) require the Holistic registered representative to document how long he or she has known the customer and under what circumstances he or she came to meet the customer.

We will review public information, including information available in Internet databases, to determine whether any "private banking" account holders are "senior foreign political figures" or close relatives thereof. If we discover information indicating that a particular private banking account holder may be a senior foreign political figure or a close relative thereof, and upon taking additional reasonable steps to confirm this information, if we determine that the individual is, in fact, a "senior foreign political figure" or a close relative thereof, 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, including 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 sources of funds, and monitoring transactions to the extent necessary to detect and report proceeds of foreign corruption, and reviewing monies coming from 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. If a higher risk is apparent, we will consider additional due diligence measures such as those described for private banking account customers above.

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, file a SAR-SF, or close the account.

In an effort to further enhance overall scrutiny of "senior foreign political figure accounts", the Firm's designated Compliance Officer on a monthly basis reviews and analyzes each account via the "AML PEP" report provided by our clearing firm. The review is conducted in order to analyze wire activity, journals and account transactions. The main purpose of this review is to detect increase or decrease of funds or asset value that is not attributable to fluctuations in the market value of the investments instruments held in the account. A copy of the account's analysis is maintained on file. Additionally, to detect frequent or excessive use of funds and/or money movement a spreadsheet is maintained illustrating overall money movement in each account during the previous quarter.

## XI. FCPA Prohibitions

The FCPA prohibits employees from presenting an offer, gift, payment, promise of payment, authorization of payment, or any item of value to a Foreign Official with the intent of assisting the Firm in obtaining, retaining or directing business to any person. Intent can include those gifts, payments, *etc.* made with a conscious disregard or deliberate ignorance of their purpose.

The FCPA also prohibits any such payments to third parties or intermediaries while knowing that all or a portion of such money or thing of value will be offered, given or promised, directly or indirectly, to any Foreign Official. Intermediaries can include, but are not limited to, joint venture partners or other agents such as consultants, independent service providers and vendors.

Cash payments and political contributions made on behalf of the Firm to Foreign Officials, either directly or via a third party, are prohibited.

### *A. Required Approvals*

An expenditure of any size for courtesies, gifts, entertainment, travel, lodging or other payment of any kind to or on behalf of any Foreign Official must be approved in accordance with the Firm's gifts Program. All questions about the application of this Program, or concerns regarding potential violations of the Program, should be directed to CCO.

### *B. Contracts With Third Parties*

The Firm must exercise reasonable due diligence in the selection of any third party to be used in connection with a foreign government, its officials or anyone meeting this Program's definition of "Foreign Official." No agent, representative, or consultant may be retained for such purpose without the written approval of CCO after the satisfactory completion of appropriate due diligence procedures. Contracts with such third parties will be in writing, and specifically bind the individual or entity to comply with the FCPA. Payment to such third parties will be permitted only if it is reasonable in relation to the services performed.

### *C. Business Entertainment, Gifts And Travel Expenses*

Entertainment, gifts and travel expenses may not be paid to, or on behalf of, Foreign Officials unless they meet all of the guidelines below. For further guidance, employees should contact CCO.

- The expenditures should not be lavish or excessive, on either a per capita or event basis, as determined by the economic standards of the country in which the benefit is being given.
- A valid business purpose should be associated with all Firm-funded activities.
- The event or provision of gifts should be infrequent.
- The event or activity should be legal under both U.S. and local law, within accepted industry norms, and consistent with Firm Program.
- The expenditures should be accurately and adequately documented in the Firm's books and records, including their business purpose, value and record of approval.
- Travel and hotel expenses for government officials should be made directly to the vendor by the Firm rather than allowing the officials to pay their own way and to seek reimbursement.
- Entertainment and gifts must comply with the Firm's policies.
- All expenditures must be permitted under the local law where the Foreign Official is employed, which may be more restrictive than U.S. law. For further guidance on complying with this requirement, employees are encouraged to confer with Compliance.

### *D. Promotional/Educational Expenses*

Reasonable promotional expenditures are permitted under the FCPA; however, they must not be designed to improperly influence a Foreign Official in a decision-making capacity. If the Firm intends to cover any of the attendee's expenses at a promotional/educational event, and one or more attendees is a Foreign Official, approval by CCO is required.

### *E. Facilitating Payments*

The FCPA's general anti-bribery prohibition does not apply to small payments to facilitate and expedite performance of a "routine governmental activity" (*i.e.,* ministerial actions to which the Firm is legally entitled), such as obtaining permits, licenses and official documents, processing governmental papers, or providing postal or utility services. "Routine governmental

action" does not include any discretionary decision by a foreign official to award new business or to continue business with the Firm.

In as much as the FCPA does not prohibit these types of facilitation payments to be made outside of the United States, local law may prohibit them. In such cases, local law will prevail. If such payments are permitted, they may be made only after written pre-approval has been obtained from CCO.

### *F. No Cash Payments To Foreign Officials*

Payments to a Foreign Official, third-party service provider, or anyone else pursuant to an available and approved exemption from the FCPA must not be made in cash. Checks may not be made payable to "cash," "bearer," or other designees of the party entitled to payment. Payments may not be made outside the country of residence of the recipient without prior consultation and approval of CCO.

### *G. Political Contributions*

Neither the Firm nor any employee should make any political contribution on behalf of the Firm to a foreign government, official, or political party or candidate in a foreign country without prior approval by CCO. Private political contributions are not under any circumstances reimbursable by the Firm.

### *H. Financial And Accounting Controls*

The Firm's FINOP/CFO is responsible for establishing appropriate accounting and financial policies, procedures and other internal controls to fulfill the accounting provisions of the FCPA. The FINOP/CFO will report any suspicious payments or patterns of suspicious payments to persons located in high risk jurisdictions to the Firm's AMLCO and/or President.

## XII. Monitoring Accounts for Suspicious Activities

Holistic will monitor on a regular basis the account activity to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as "non-cooperative" are involved, or any of the "red flags" identified. We will look at transactions, including trading and wire transfers, in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that customer. The AML Compliance Officer or her designees 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 it is carried out, and will report suspicious activities to the appropriate authorities. We will document our monitoring and reviews.

Among the information we will use to determine whether to file a Form SAR-SF are exception reports (see section XV for specific exception reports utilized) that include transaction

size, location, type, number, and nature of the activity. Our AML Compliance Officer will conduct an appropriate investigation before a SAR-SF is filed.

To further enhance our scrutiny of suspicious activities, the AMLCO reviews the Electronic Compliance Surveillance platform ("Actimize") provided by Pershing, LLC and retrieves the money activity for all accounts on a monthly basis to detect activity that might appear to be out of the ordinary. The monthly activity is sorted by account. This allows for further review of individual accounts that could be active or receiving funds from unknown sources.

Whenever a request to disburse funds is received, the broker is asked to provide a reason for the disbursement and the relationship to the beneficiary. An OFAC search is performed on all third-party beneficiaries. The activity for the account is then reviewed in order to detect possible suspicious movements prior to approval of the disbursement.

Any unusual or suspicious transactions resulting from such monitoring shall be referred to the AML Compliance Officer for a determination as to whether a suspicious activity report on SAR-SF is appropriate. The Firm utilizes Actimize to further enhance and conduct suspicious activity monitoring.

## XIII. Emergency Notification to Law Enforcement by Telephone

When conducting due diligence or opening an account, we will immediately call Federal law enforcement when necessary, and especially in these emergencies: a legal or beneficial account holder or person with whom the account holder is engaged in a transaction is listed on or located in a country or region listed on the OFAC list, an account is held by an entity that is owned or controlled by a person or entity listed on the OFAC list, a customer tries to use bribery, coercion, or similar means to open an account or carry out a suspicious activity, we have reason to believe the customer is trying to move illicit cash out of the government's reach, or we have reason to believe the customer is about to use the funds to further an act of terrorism. We will first call the OFAC Hotline at 1-800-540-6322. The other contact numbers we will use are: Financial Institutions Hotline (1-866-556-3974), local U.S. Attorney's Office (305) 961-9000, local FBI Office (305) 944-9101 and local SEC Office (305) 982-6300.

## XIV. Red Flags

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

### Customers – Insufficient or Suspicious Information

- Provides unusual or suspicious identification documents that cannot be readily verified.

- Reluctant to provide complete information about nature and purpose of business, prior banking relationships, anticipated account activity, officers and directors or

business location.

- Refuses to identify a legitimate source for funds or information is false, misleading or substantially incorrect.

- Background is questionable or differs from expectations based on business activities.

- Customer with no discernable reason for using the firm's service.

**Efforts to Avoid Reporting and Recordkeeping**

- Reluctant to provide information needed to file reports or fails to proceed with transaction.

- Tries to persuade an employee not to file required reports or not to maintain required records.

- "Structures" deposits, withdrawals or purchase of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements.

- Unusual concern with the firm's compliance with government reporting requirements and firm's AML policies.

**Certain Funds Transfer Activities**

- Wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent business reason.

- Many small, incoming wire transfers or deposits made using checks and money orders. Almost immediately withdrawn or wired out in manner inconsistent with customer's business or history. May indicate a Ponzi scheme.

- Wire activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.

**Certain Deposits or Dispositions of Physical Certificates**

- Physical certificate is titled differently than the account.

- Physical certificate does not bear a restrictive legend, but based on history of the stock and/or volume of shares trading, it should have such a legend.

- Customer's explanation of how he or she acquired the certificate does not make sense or changes.

- Customer deposits the certificate with a request to journal the shares to multiple accounts, or to sell or otherwise transfer ownership of the shares.

**Certain Securities Transactions**

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

**Transactions Involving Penny Stock Companies**

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

**Transactions Involving Insurance Products**

- Cancels an insurance contract and directs funds to a third party.
- Structures withdrawals of funds following deposits of insurance annuity checks signaling an effort to avoid BSA reporting requirements.

- Rapidly withdraws funds shortly after a deposit of a large insurance check when the purpose of the fund withdrawal cannot be determined.

- Cancels annuity products within the free look period which, although could be legitimate, may signal a method of laundering funds if accompanied with other suspicious indicia.

- Opens and closes accounts with one insurance company then reopens a new account shortly thereafter with the same insurance company, each time with new ownership information.

- Purchases an insurance product with no concern for investment objective or performance.

- Purchases an insurance product with unknown or unverifiable sources of funds, such as cash, official checks or sequentially numbered money orders.

**Activity Inconsistent With Business**

- Transactions patterns show a sudden change inconsistent with normal activities.

- Unusual transfers of funds or journal entries among accounts without any apparent business purpose.

- Maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.

- Appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.

**Other Suspicious Customer Activity**

- Unexplained high level of account activity with very low levels of securities transactions.

- Funds deposits for purchase of a long-term investment followed shortly by a request to liquidate the position and transfer the proceeds out of the account.

- Law enforcement subpoenas.

- Large numbers of securities transactions across a number of jurisdictions.

- Buying and selling securities with no purpose or in unusual circumstances (e.g., churning at customer's request).

- Payment by third-party check or money transfer without an apparent connection to

the customer.

- Payments to third-party without apparent connection to customer.

- No concern regarding the cost of transactions or fees (i.e., surrender fees, higher than necessary commissions, etc.).

* * * *

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 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 filing a SAR-SF.

## XV. Ongoing Customer Due Diligence

The Firm identifies certain accounts that are subject to enhanced due diligence (i.e. charity, non-for profit, PEP, foreign financial institution, and tax heaven accounts), which require conducting a review at least on a yearly basis or as necessary. The enhanced review will identify suspicious activity, red flags and an assessment of customers' activity review (i.e. trading and assets movements) vs information gathered as part of the Firm's Know Your Client process. The Legal Entity Certification, which identifies beneficial owners of legal entity owners will also be updated. If information in records is deemed outdated, the Firm will update any relevant data as required. If necessary, the account will be subject to an AML Investigation which might result in specific actions such as limitations, restrictions, etc. and if appropriate, a SAR filling.

## XVI. Suspicious Transactions and BSA Reporting

Should any employee of Holistic, or any clearing broker used by Holistic, detect any suspicious activity which appears to involve money laundering with respect to a customer of Holistic, such person or entity shall contact the AML Compliance Officer. The AML Compliance Officer, after consulting with senior management shall determine the appropriate course of action to take with respect to the suspicious activity including any necessity to block or freeze the account, or to report the suspicious activity to federal authorities on Form SAR-SF and to notify the clearing firm. If a SAR-SF is filed with FinCEN, the AML Compliance Officer will promptly notify the Managing Partners of Holistic. The AML Compliance Officer shall also notify any employee involved of the confidential nature of the information contained in such report.

## XVII. Filing a Form SAR-SF

Holistic will file Form SAR-SFs for any account activity (including deposits and transfers) conducted or attempted through our firm involving (or in the aggregate) $5,000 or more of funds or assets where we know, suspect, or have reason to suspect that the; (a) 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, (b) the transaction is designed, whether through structuring or otherwise, to evade the requirements of the BSA regulations, (c) 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 we know, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the transaction, or (d) the transaction involves the use of the firm to facilitate criminal activity.

We will also file a SAR-SF 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-SF we have filed may require immediate attention by the SEC. 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-SF reporting the violation.

We will report to the SEC or SRO if a violation occurs regarding Federal securities laws or SRO rules by our employees or registered representatives that do not involve money laundering or terrorism.

We may file a voluntary SAR-SF 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 SAR-SFs will be reported regularly to the Board of Managers of the Firm and appropriate senior management, with a clear reminder of the need to maintain the confidentiality of the SAR-SF.

We will report suspicious transactions by completing a SAR-SF, and we will collect and maintain supporting documentation as required by the BSA regulations. The Firm will file a SAR-SF no later than thirty (30) calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR-SF. If no suspect is identified on the date of initial detection, the Firm may delay filing the SAR-SF for an additional 30 calendar days pending identification of a suspect, but in no case, will the reporting be delayed more than sixty (60) calendar days after the date of initial detection. In accordance with reflected industry practice the SAR determination ("The time period for filing a SAR starts when Holistic through its review or because of other factors, knows or has reason to suspect that the activity or transactions under review meet one or more of the definitions of suspicious activity." [6] As such the "initial detection" is not reflected by 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. The Firm may document its initial detection date and its overall review

[6] Bank Secrecy Act Advisory Group, "Section 5 — Issues and Guidance," The SAR Activity Review – Trends, Tips & Issues, Issue 10, May 2006, page 44, at www.fincen.gov

timeframe in various manners including, but not limited to: Interoffice Memorandum and AML monitoring log.

We will report suspicious transactions by completing a SAR-SF 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-SF. If no suspect is identified on the date of initial detection, we may delay filing the SAR-SF for an additional 30 calendar days pending identification of a suspect, but in no case, will the reporting be delayed more than 60 calendar days after the date of initial detection.

We will retain copies of any SAR-SF filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR-SF. Copies all any SAR-SF filed will be retained in a secured cabinet in the CCO's office. We will identify and maintain supporting documentation and make such information available to FinCEN, any other appropriate law enforcement agencies, or federal or state securities regulators or FINRA, 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-SF or the information contained in the SAR-SF, except where disclosure is requested by FinCEN, the SEC, or another appropriate law enforcement or regulatory agency or an SRO registered with the SEC, will decline to produce the SAR-SF or to provide any information that would disclose that a SAR-SF was prepared or filed. We will notify FinCEN of any such request and our response.

## XVIII. Reporting Movements of Money

Pursuant to the BSA, the Firm is required to file a Currency Transaction Report ("CTR") with the IRS Detroit Computing Center (which processes them on behalf of the Director of the Treasury's Financial Crimes Enforcement Network or "FinCEN") for deposits, withdrawals, exchanges of currency (i.e., coin or paper money), or other payments or transfers involving a transaction in currency, totaling $10,000 or more in one business day. With respect to currency transactions, multiple transactions must be treated as a single transaction if the Firm has knowledge that they are by or on behalf of the same person, and they result in either currency received (cash in) totaling more than $10,000 in any one business day. This applies to any partner, director, officer, or employee of the Firm, or any existing system at the Firm that permits the firm to aggregate transactions. We will use the Currency transaction Form ("CTR") provided by BSA.

Another requirement of the BSA, but reported to the Commissioner of Customs on a Currency and Monetary Transportation Report ("CMIR"), is the reporting of transactions involving the movement of currency or monetary instruments (i.e., traveler's checks and all negotiable instruments, including personal and business checks, official bank checks, cashier's checks, third-party checks, promissory notes, money orders, or securities in bearer form) over $10,000 into or out of the U.S.

It is the Program of the Firm that currency will neither be received nor disbursed, nor will the Firm disburse monetary instruments. The operational staff will notify the AML Compliance Officer whenever the Firm is in receipt of a foreign monetary instrument in excess of $10,000, or if a customer requests a monetary instrument in excess of $10,000 to be sent outside of the U.S. (even when such shipment or transport is made by the Firm to an office of the Firm located outside the U.S.). The AML Compliance Officer will then be responsible for determining whether the Firm should receive or disburse such funds and documenting the circumstances and the reasons for the approval or rejection.

A third requirement of the BSA is, if a broker-dealer has a financial interest in or signature authority over a financial account in a foreign country, it must be reported on a Report of Foreign Bank and Financial Accounts ("FBAR") to FinCEN if the aggregate value exceeds $10,000. The Firm's AML Compliance Officer will be responsible for completing the Treasury Department Form TD F 90-22.1, *Report of Foreign Bank and Financial Accounts,* and file such report with FinCEN. The report must be filed each calendar year on or before June 30. The Designated Supervisor shall, prior to June 30 of each year, assess whether the Firm is required to file the FBAR form and shall make any appropriate filings. The Firm will maintain all FBAR filings for a minimum of five years.

Though it is the Firm's Program not to accept cash deposits, the following procedures have been created in the event an employee inadvertently accepts cash.

If a customer attempts to deposit cash or currency, the employee receiving the deposit is responsible for refusing the deposit and advising the customer Holistic will only accept checks.

In the event cash is inadvertently accepted, the following steps must be followed:

- Immediately provide the cash to the cashier or other authorized Operations personnel.
- The CCO is responsible for counting the cash (2 people must be present to verify the amount) and entering the amount into Holistic's customer account system for credit to the customer's account.
- Immediately thereafter the cash must be walked to Holistic's bank for credit to the account maintained for the benefit of customers or, if no account exists, obtain a cashier's check or money order made payable to the clearing firm and then send the check/money order to the clearing firm the same day.
- The CCO is responsible for filing Form 4789 (Currency Transaction Report) with the IRS by the 15$^{th}$ calendar day after receipt for cash in excess of $10,000 for one person on any one day.
- The CCO is responsible for retaining a file of forms filed with the IRS.

## XIX. Transfers of $3,000 or More Under the Joint and Travel Rule

When we transfer funds of $3,000 or more, we will record on the transmittal file at least the following information: the name and address of the transmitter, the amount of the transmittal order along with the execution date, the identity of the transmitter's financial institution, and the account number of the transmitter, a copy of the transmitter's account profile will be added to the transmittal file. We will also record the identity of the recipient's financial institution.

For all third-party transmittals we will check the recipient's name on OFAC and World-Check or LexisNexis before the payment is authorized, copies of the results will be attached to the transmittal file.

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.

## XX. Law Enforcement Requests to Maintain Accounts Open

This Section XX provides the procedures for Holistic to follow with respect to account relationships that law enforcement may have an interest in ensuring remain open notwithstanding suspicious or potential criminal activity in connection with the account. Ultimately, the decision to maintain or close an account should be made by Holistic. Although there is no requirement that Holistic maintain a particular account relationship, Holistic should be mindful that complying with such a request may further law enforcement efforts to combat money laundering, terrorist financing, and other crimes.

If a law enforcement agency requests that Holistic maintain a particular account, Holistic shall ask the requesting law enforcement agency to memorialize its request in writing. A written request from a federal law enforcement agency should be issued by a supervisory agent or by an attorney within a United States Attorney's Office or another office of the Department of Justice. If a state or local law enforcement agency requests that an account be maintained, then Holistic should obtain a written request from a supervisor of the state or local law enforcement agency or

from an attorney within a state or local prosecutor's office. The written request should indicate that the agency has requested that Holistic maintain the account and the purpose of the request. For example, if a state or local law enforcement agency is requesting that Holistic maintain the account for purposes of monitoring, the written request should include a statement to that effect. The request should also indicate the duration for the request, not to exceed six months. Although there is no recordkeeping requirement under the Bank Secrecy Act for this type of correspondence, pursuant to FinCEN guidance (see FinCEN, Guidance, FIN-2007-G002 (June 13, 2007)), FinCEN recommends that a securities broker-dealer such as Holistic maintain documentation of such requests for at least five years after the request has expired. If MCMs aware – through a subpoena, 314(a) request, National Security Letter, or similar communication – that an account is under investigation, FinCEN has recommended that a securities broker-dealer such as Holistic should notify law enforcement before making any decision regarding the status of the account.

If Holistic chooses to maintain the account in light of a law enforcement request to maintain the account open, Holistic is still required to comply with all applicable Bank Secrecy Act recordkeeping and reporting requirements, including the requirement to file SARs, even if Holistic is keeping an account open or maintaining a customer relationship at the request of law enforcement.

## XXI. AML Record-Keeping

### *A. Responsibility for Required AML Records and SAR-SF Filing*

Our AML Compliance Officer will be responsible for ensuring that AML records are maintained properly and that SAR-SFs are filed as required.

In addition, as part of our AML program, our firm will create and maintain SAR-SFs, CTRs, CMIRs, FBARs, and relevant documentation on customer identity and verification *(See* CIP above) and funds transmittals. We will maintain SAR-SFs and their accompanying documentation for at least five (5) 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 (6) 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)).

### *B. SAR-SF Maintenance and Confidentiality*

We will hold SAR-SFs and any supporting documentation confidential. We will not inform anyone outside of FinCEN, the SEC, and SRO registered with the SEC or other appropriate law enforcement or regulatory agency about a SAR-SF. We will refuse any subpoena requests for SAR-SFs or for information that would disclose that a SAR-SF 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-SF filings and copies of supporting documentation from other firm books and records to avoid disclosing SAR-SF filings. Our AML Compliance Officer will handle all subpoenas or other requests for SAR-SFs. 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.

### *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.

## XXII. Clearing Firm/Introducing Firm Relationships

We will work closely with our clearing firms, Pershing & RBC Correspondent Services, 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. As a general matter, we will obtain and use a variety of exception reports offered by our clearing firm, which are outlined throughout the Firm's AML procedures. In addition, the Firm utilizes a number of other clearing firm exception reports to monitor various activities, which is outlined and maintained under a separate cover. The Firm provides its 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.

.

## XXIII. Training of Our Employees

We will have ongoing employee discussions under the leadership of the AML Compliance Officer and senior management to discuss any new AML regulations and procedures to ensure that our registered representatives and management understand these important matters. Our training will occur on at least an annual basis in conjunction with our annual compliance meeting. 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 SAR-SFs); (3) what employees' roles are in the firm's compliance efforts and how to perform them; (4) the Firm's record retention program; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the PATRIOT Act.

We will develop training at the Firm, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos. We will maintain records to show the persons trained the dates of training, and the subject matter of their training.

Holistic will review our operations to see if certain employees require specialized additional training. Our written procedures will be updated to reflect any such changes.

## XXIV. Program to Independently Test AML Program

As a general matter, the scope of independent testing of the Firm's AML compliance program should include: (1) evaluating the overall integrity and effectiveness of the Firm's AML compliance program; (2) evaluating the Firm's procedures for BSA reporting and recordkeeping

requirements; (3) evaluating the implementation and maintenance of the Firm's CIP; (4) evaluating the Firm's customer due diligence requirements; (5) evaluating the Firm's transactions, with an emphasis on high-risk areas; (6) evaluating the adequacy of the Firm's staff training program; (7) evaluating the Firm's systems, whether automated or manual, for identifying suspicious activity; (8) evaluating the Firm's system for reporting suspicious activity; and (9) evaluating the Firm's response to previously identified deficiencies.

### *A. Staffing*

The testing of our AML Program will be performed at least annually (on a calendar year basis) by an independent third-party consulting firm. We will evaluate the qualifications of the independent third party to ensure they have a working knowledge of applicable requirements under the BSA and its implementing regulations. Independent testing will be performed more frequently if circumstances warrant.

### *B. Evaluation and Reporting*

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

## XXV. Monitoring Employee Conduct and Accounts

Holistic 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 the Firm's President.

## XXVI. Confidential Reporting of AML Non-Compliance

Employees will report any 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 their designated supervisor. Such reports will be confidential, and the employee will suffer no retaliation for making them.

Holistic will have an independent test (as that term is used in and interpreted under the USA PATRIOT Act of 2001) of its AML program at least annually. Such test shall be conducted by a person knowledgeable regarding the BSA requirements then in effect. The test may be conducted by a person who is an affiliate of Holistic, or by an unaffiliated person; provided that the person conducting the test is not involved in the operation or oversight of Holistic' AML program. A written assessment or report of such independent test, including any recommendations from such review, shall be provided to the senior management of Holistic in connection with their review of the adequacy of this Program. Copies of this Program, any amendments to this Program, any reports made to authorities of currency transactions or

suspicious activities, reports on the independent test and any recommendations made to the Firm's senior management shall be kept in the files for at least five (5) years.

The senior management of Holistic shall review and approve this Program no less frequently than annually. Holistic and its senior management are firmly committed to compliance with all laws and regulations relating to combating money laundering and terrorist financing, including laws that criminalize money laundering and rules and regulations requiring reporting of currency transactions, certain monetary instruments and suspicious activity.

Protecting Holistic against exploitation by money launders is the responsibility of every employee. Any involvement in money laundering, even if unintentional or indirect, through association with a customer that is involved in such activities could result in serious civil and criminal penalties for the Firm and its employees, as well as forfeiture of assets. Association with money laundering also could cause significant damage to Holistics' reputation.

Under no circumstance may an employee of Holistic, willfully facilitate or participate in any money laundering activity. Any violation of this Program will subject the employee involved to disciplinary action, including dismissal, and may subject them to possible civil and criminal penalties.

Holistic has adopted this Program to assist its employee to guard against money laundering through the Firm and to encourage employees to detect and report transactions as required by the Government.

## XXVII. Senior Manager Approval

I have approved this AML Program as reasonably designed to achieve and monitor the Firm's ongoing compliance with the requirements of the BSA and the implementing regulations under it.

Gustavo Dominguez Digitally signed by Gustavo Dominguez
Date: 2022.05.18 14:39:50 -04'00'

Signed: _____
Name: Gustavo Marcelo Dominguez
Title: CCO

Date: May 18th, 2022