AML Policy

Smart MFG Tech LTD.

Anti-Money Laundering (AML) Program:

Compliance and Supervisory Procedures

1. Smart MFG Tech LTD. Policy

It is the policy of Smart MFG Tech LTD. CO. (Smart MFG Tech LTD.) 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 UK Proceeds of Crime Acts, The Terrorism Act, the Bribery Act, the Money Laundering Regulations of EU the FCA Rules and Guidance, the U.S. Bank Secrecy Act (BSA).

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in

three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Although cash is rarely deposited into crypto currency accounts, the industry is unique in that it can be used to launder funds obtained elsewhere, and to generate illicit funds within the industry itself through fraudulent activities. Examples of types of fraudulent activities include ponzi schemes, cybercrime and other fraudulent activity.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate

sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds.
Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.
Our AML policies, procedures and internal controls are designed to ensure compliance with UK, EU, U.S. BSA regulations and FINRA rules and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

2. AML Compliance Person Designation and Duties

Designate your firm's AML Compliance Person and describe his or her duties.

Smart MFG Tech LTD. has designated legal counsel as its temporary Anti-Money Laundering Program Compliance (AML Compliance Person), with responsibility for the firm's AML program until such time as a full-time Compliance Officer can be hired. The duties of the AML Compliance Person will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees. The AML Compliance Person will also ensure that the firm keeps and maintains all of the required AML records and will ensure that Suspicious Activity Reports or Notices are filed with the UK authorities and, if applicable, the U.S. Financial Crimes Enforcement Network (FinCEN) when appropriate. The AML Compliance Person is vested with full responsibility and authority to enforce the Smart MFG Tech LTD.'s AML program.

If so required, Smart MFG Tech LTD. will provide the relevant reporting agencies with contact information for the AML Compliance Person and will, if relevant, through the U.S. FINRA Contact System (FCS), including: (1) name; (2) title; (3) mailing address; (4) email address; (5) telephone number; and (6) facsimile (if any). If applicable, Smart MFG

Tech LTD. will promptly notify a relevant agency of any changes review, and if necessary update, this information after the end of each calendar year.

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

A) Requests for Information by Authorities

We will respond to a request from law enforcement and regulatory agencies concerning accounts and transactions by immediately searching our records to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity or organization named in the Request. We understand that we have a limited time from the transmission date of the request to respond to a Request by such an authority. If we find a match, our then in-effect Compliance Officer will report it to the relevant agency in the time so specified. The search we conduct will be structured according to the request.

If the Smart MFG Tech LTD. Compliance Officer searches our records and does not find a matching account or transaction, then Smart MFG

Tech LTD. will not respond to the request. We will maintain documentation that we have performed the required search by maintaining a log showing the date of the request, the number of accounts searched, the name of the individual conducting the search and a notation of whether or not a match was found.

We will not disclose the fact that a law or regulatory authority has requested or obtained information from us, except to the extent necessary to comply with the information request. Smart MFG Tech LTD.'s Compliance Officer will review, maintain and implement procedures to protect the security and confidentiality of requests from a law enforcement or regulatory agency with regard to the protection of customers' nonpublic information.

We will direct any questions we have about any Request for information to the requesting law enforcement or regulatory agency as designated in the request.

Unless otherwise stated in a Request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the periodic Requests as a government provided list

of suspected terrorists for purposes of the customer identification and verification requirements.

B) National Security Letters

Smart MFG Tech LTD. understands that the receipt of a FCA request, a UK AML, or CTF or a U.S. National Security Letter (NSL) is highly confidential. We understand that none of our officers, employees or agents may directly or indirectly disclose to any person that a law enforcement or government authority has sought or obtained access to any of our records. To maintain the confidentiality of any request we receive, we will process and maintain the NSL by segregating the request and disclosing on a need to know only basis and with as limited disclosure on such a basis and securing such requests and information derived therefrom on a secure basis. If we file a response after receiving such a response the response, will not contain any reference to the receipt or existence of the request. The Response will only contain detailed information about the facts and circumstances of the detected suspicious activity.

C) Subpoenas

We understand that the receipt of a subpoena from a court concerning a customer does not in itself require that we file a Suspicious Activity or other report. When we receive a subpoena, we will conduct a risk assessment of the customer subject to the subpoena as well as review the customer's account activity. If we uncover suspicious activity during our risk assessment and review, we will elevate that customer's risk assessment and file a response in accordance with the applicable requirements. We understand that none of our officers, employees or agents may directly or indirectly disclose to the person who is the subject of the subpoena its existence, its contents or the information we used to respond to it. To maintain the confidentiality of any grand jury subpoena we receive, we will process and maintain the subpoena by segregating the request and disclosing on a need to know only basis and with as limited disclosure on such a basis and securing such requests and information derived therefrom on a secure basis. If we file a report after receiving a subpoena, the report will not contain any reference to the receipt or existence of the subpoena. The report will only contain detailed information about the facts and

circumstances of the detected suspicious activity. Subpoenas or other demands for information that arise in a civil, non-law enforcement or national security context will not be responded to until such time as a competent court may order such disclosure.

4. Checking the Office of Foreign Assets Control Listings

Before purchasing MFG Token, and on an ongoing basis, our Compliance Officer will check to ensure that a customer does not appear on a Specially Designation Nationals list (SDN) or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by a relevant authority such as the U.S. OFAC. Because the SDN list and listings of economic sanctions and embargoes are updated frequently, we will consult them on a regular basis and subscribe to receive any available updates when they occur. With respect to the SDN list, we may also access that list through various software programs to ensure speed and accuracy. If applicable, the Smart MFG Tech LTD. Compliance Officer will also review existing accounts against the SDN list and

listings of current sanctions and embargoes when they are updated and he/she will document the review.

If we determine that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by a controlling authority, we will reject the transaction and/or block the customer's assets and file a blocked-assets, and/or rejected transaction report, as may be required.

Our review will include customer accounts, transactions involving customers (including activity that passes through the firm such as wires).

5. Customer Identification Program

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

appropriate procedures if a potential or existing customer either refuses to provide the information in our Know your Customer (KYC) request, or appears to have intentionally provided misleading information, Smart MFG Tech LTD. will not and, after considering the risks involved, consider closing any existing account/transactions. In either case, our AML Compliance Person will be notified so that we can determine whether we should report the situation to a relevant authority.

A) Refusal to Provide Information

If a potential or existing customer either refuses to provide the information in our Know your Customer (KYC) request, or appears to have intentionally provided misleading information, Smart MFG Tech LTD. will not and, after considering the risks involved, consider closing any existing account/transactions. In either case, our AML Compliance Person will be notified so that we can determine whether we should report the situation to a relevant authority.

B) Verifying Information

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. Smart MFG Tech LTD.'s Compliance Officer will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).

We will verify customer identity through documentary means, non-documentary means or both using the Identity Mind Global KYC compliance platform. In addition, will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. We may also use non-documentary means, if we are still uncertain about whether we know the true identity of the customer. In verifying the information, we

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

Appropriate procedures and documents for verifying the identity of customers may include some or all of the following:

- Create an Account with a User ID and Password;
- Background Check, OFAC, PEP, Interpol, FBI, DEA and additional databases;
- Two-Factor authentication via SMS to verify cellular number;
- Review of Government Issued Identification (Driver License/Passport); and
- Biometric facial recognition.

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

can form a reasonable belief that we know the customer’s true identity.

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

- Independently verifying the customer’s identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source such as the OFAC SDN list
- Checking references with other financial institutions; or
- Obtaining a financial statement.

We will verify the information within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or the value 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 Smart MFG Tech LTD.'s AML Compliance Person, file a report accordance with applicable laws and regulations.

We recognise that the risk that we may not know the customer's true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated as a primary money laundering or suspicious 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.

C) Lack of Verification

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

D) 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 the required period of time after the record is made.

E) Comparison with Government-Provided Lists of Terrorists

If 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 AML or security 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 government agency and designated as such by a banking or regulatory authority. We will follow all directives issued in connection with such lists.

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

F) Notice to Customers

We will provide notice to customers that Smart MFG Tech LTD. is requesting information from them to verify their identities, as required by federal law. We will use the following method to provide notice to customers: via notice on the Smart MFG Tech LTD. website and when

a customer attempts to enter a transaction, notice of our KYC process will be posted.

Important Information About Procedures for Opening a New Account

To help the government fight the funding of terrorism and money laundering activities, law requires us to obtain, verify, and record information that identifies each person who engages in a transaction. What this means for you: When you engage in a transaction, 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.

G) Reliance on Another Financial Institution for Identity Verification

We may, under the following circumstances, rely on the performance by another entity for some or all of the elements of our AML with respect to any customer before we provide or engage in services, dealings or other financial transactions.

6. Customer Due Diligence Rule

In addition to the information collected under KYC rules we have established, documented and maintained written policies and

procedures reasonably designed to identify and verify beneficial owners of legal entity customers and comply with other aspects of the Customer Due Diligence. We will collect certain minimum CDD information from beneficial owners of legal entity customers. We will understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile. We will conduct ongoing monitoring to identify and report suspicious transactions, and, on a risk basis, maintain and update customer information.

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

(1) the name;

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

(3) an address, which will be a residential or business street address (for an individual), a PO Box number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address); and

(4) an identification number, which will be a government issued tax ID number, or one or more of the following: a passport number and country of issuance, or other similar identification number, such as an alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard.

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

In the event that a beneficial owner of a legal entity customer has applied for, but has not received, a tax ID number or a passport number or other similar identification number, we will use a 3d party

KYC process to confirm that the application was filed before the customer opens the account and to obtain the applicable identification number within a reasonable period of time after the account is opened.

B) Understanding the Nature and Purpose of Customer Relationships

We will understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile through the following methods 3d party multi part KYC process which may include bio-metric processes.

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

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

C) Conducting Ongoing Monitoring to Identify and Report Suspicious Transactions

We will conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, maintain and update customer information, including information regarding the beneficial ownership of legal entity customers, using the customer risk profile as a baseline against which customer activity is assessed for suspicious transaction reporting.

7. Monitoring Accounts for Suspicious Activity

We will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and “red flags” that are appropriate to our business. Monitoring will be conducted through the following methods: unusually large transactions, requests for special consideration or shortened KYC requests. The customer risk profile will serve as a baseline for assessing potentially suspicious activity. The AML Compliance Person or his or her designee will be responsible for this monitoring, will review any activity that our monitoring system detects, will determine whether any additional steps are required, will document when and how this

monitoring is carried out, and will report suspicious activities to the appropriate authorities

A) Emergency Notification to Law Enforcement by Telephone

In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, we will immediately call an appropriate law enforcement authority.

B) Red Flags

Red flags or warnings of activity 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 Transactions

- Customer has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason.

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.).

C) Responding to Red Flags and Suspicious Activity

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

8. Suspicious Transactions and Reporting

When an employee of the firm detects any suspicious transaction, or other activity that may be suspicious, he or she will notify our Compliance Officer, then an Officer of the Company. Under the direction of the AML Compliance Person, the firm will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or filing a report with the relevant authority.

A) Filing a Suspicious Activity Report

We will file suspicious activity report for any transactions conducted or attempted by, at or through our firm involving $5,000 or more of funds or assets (either individually or in the aggregate) where we know, suspect or have reason to suspect:

(1) the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal

law or regulation or to avoid any transaction reporting requirement under federal law or regulation;

(2) the transaction is designed, whether through structuring or otherwise, to evade any requirements of an applicable regulation;

(3) the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction; or

(4) the transaction involves the use of the firm to facilitate criminal activity.

We will also file a report and notify the appropriate law enforcement authority in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes.

We may file a voluntary report 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 a rule or regulation. It is

our policy that all reports will be reported regularly to the Board of Directors and appropriate senior management, with a clear reminder of the need to maintain the confidentiality of reports.

We will report suspicious transactions by completing a report, and we will collect and maintain supporting documentation as required by regulations.

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

We will not notify any person involved in the transaction that the transaction has been reported. We understand that anyone who is subpoenaed or required to disclose a report or the information contained in the report will, except where disclosure is requested by an appropriate law enforcement or regulatory agency, decline to produce the report or to provide any information that would disclose

that a report was prepared or filed. We will notify the appropriate authority of any such request and our response.

B) Currency Transaction Reports

If so required by applicable law, we prohibit transactions involving cash transactions over €10,000 and has the following procedures to prevent such transactions: delay execution of the transaction for 24 hours or until such time as an AML and/or KYC review shows the transaction not to be suspicious. If we discover such transactions have occurred, we will file with FinCEN CTRs for currency transactions that exceed €10,000. Also, we will treat multiple transactions involving currency as a single transaction for purposes of determining whether to file a report if they total more than €10,000 and are made by or on behalf of the same person during any one business day.

C) Currency Transaction Reports

We prohibit both the receipt of currency or other monetary instruments that have been transported, mailed or shipped to us from outside of the country we are registered in, and the physical transportation, mailing or shipment of currency or other monetary

instruments by any means other than through the postal service or by common carrier. if We will file a report if we discover that we have received or caused or attempted to receive from outside of the country we are registered in, currency or other monetary instruments in an aggregate amount exceeding €10,000 at one time (on one calendar day or, if for the purposes of evading reporting requirements, on one or more days).

D) Monetary Instrument Purchases

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

9. AML Recordkeeping

A) Responsibility for Required AML Records and Report Filing

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

In addition, as part of our AML program, our firm will create and maintain suspicious activity reports and relevant documentation on customer identity and verification and funds transmittals. We will

maintain suspicious activity reports and their accompanying documentation as required by law.

B) SAR-SF Maintenance and Confidentiality

We will hold suspicious activity reports and any supporting documentation confidential. We will not inform anyone outside of an appropriate law enforcement or regulatory agency about a suspicious activity report or information request. We will refuse any subpoena requests for such reports and requests or for information that would disclose that a report or response to a request for information has been prepared or filed and immediately notify the relevant authority of any such subpoena requests that we receive. We will segregate reports and requests for information filings and copies of supporting documentation from other firm books and records to avoid disclosing any such filings. Our AML Compliance Person will handle all subpoenas or other requests for any reports or requests for information. Our records of any reports or requests for information will be kept in digital form separated from our business records.

C) Additional Records

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

- If so required by law, 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 UK.

10. Training Programs

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

Our training will include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees’ duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, the filing of reports; (3) what employees' roles are in the firm's compliance efforts

and how to perform them; (4) the firm's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with applicable rules and regulations.

We will develop training in our firm, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos. Currently our training program is a briefing by our Compliance Officer until such time as formal training program can be established.

11. Monitoring Employee Conduct and Accounts

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

12. Confidential Reporting of AML Non-Compliance

Employees will promptly report any potential violations of the firm’s AML compliance program to the AML Compliance Person, unless the

violations implicate the AML Compliance Person, in which case the employee shall report to the Compliance Officer and the CEO. Such reports will be confidential, and the employee will suffer no retaliation for making them.

13. Senior Manager Approval

Senior management has approved this AML compliance program in writing as reasonably designed to achieve and monitor our firm’s ongoing compliance with the requirements of the BSA and the implementing regulations under it.