QUIFAS EXCHANGE

AML Policy

2018

1. Firm Policy

It is the policy of Quifas Inc., a company incorporated in the Seychelles on the 14th day of February 2018, registration number No. 202182 and having its registered office at Suite 1, Second Floor, Sound & Vision House, Francis Rachel Str., Victoria, Mahe, Seychelles 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 of Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Guidelines.

Generally speaking, the money laundering process consists of three “stages”:

Placement: The introduction of illegally obtained monies or other valuables into financial or nonfinancial institutions.

Layering: Separating the proceeds of criminal activity from their source through the use of layers of complex financial transactions. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity.

Integration: Placing the laundered proceeds back into the economy in such a way that they reenter the financial system as apparently legitimate funds.

These “stages” are not static and overlap broadly. Financial institutions may be misused at any point in the money laundering process.

Quifas Inc., a company incorporated in the Seychelles on the 14th day of February 2018, registration number No. 202182 and having its registered office at Suite 1, Second Floor, Sound & Vision House, Francis Rachel Str., Victoria, Mahe, Seychelles (hereinafter called “The Company” or “The Firm”) is committed to the highest standards of anti-money laundering (AML) compliance and requires management and employees to adhere to these standards to prevent use of our products and services for money laundering purposes. The Company will examine its Anti Money Laundering strategies, goals and objectives on an ongoing basis and maintain an effective Anti-Money Laundering program for the Company’s business that reflects the best practices for a diversified, global financial company.

Adherence to the Companies Anti-Money Laundering Program is the responsibility of all employees. The program includes client screening and monitoring requirements, “know your customer” policies (including the requirement to establish the identity of beneficial owners), Embargo policies, record keeping requirements, the reporting of suspicious circumstances in accordance with relevant laws, and training.

2. AML Compliance Person

Quifas Inc., a company incorporated in the Seychelles on the 14th day of February 2018, registration number No. 202182 and having its registered office at Suite 1, Second Floor, Sound & Vision House, Francis Rachel Str., Victoria, Mahe, Seychelles has designated its Compliance Officer (CO) as its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the firm’s AML program. CO has a working knowledge of compliance requirements and its implementing regulations and is qualified by experience, knowledge and training. The duties of the AML Compliance Person will include monitoring the firm’s compliance with AML obligations, overseeing communication and training for employees. The AML Compliance Person will also ensure that the firm keeps and maintains all of the required AML records and will ensure that Suspicious transaction reports (STR) in Seychelles are filed with the regulatory body when appropriate. The AML Compliance Person is vested with full responsibility and authority to enforce the firm’s AML program.

The firm will provide the Authorities with contact information for the AML Compliance Person,

including: (1) name; (2) title; (3) mailing address; (4) email address; (5) telephone number; and (6) facsimile number. The firm will promptly notify the Authority of any change in this information and will review, and if necessary update, this information within 14 business days after the end of each calendar year. In addition, if there is any change to the information, CO will update the information promptly, but in any event not later than 30 days following the change.

3. Overview of potential Risks in Cryptocurrencies Market

The wholesale markets comprise exchanges and dealing arrangements that facilitate the trading (buying and selling) of digital cryptographic assets some of which *may be* investment products and hedging instruments ("Traded products") including but not limited to:

- Securities: equities fixed income warrants and investment funds (Exchange Traded Funds — ETFs);
- Money market instruments: foreign exchange interest rate products term deposits;
- Financial derivatives: options futures swaps and warrants;
- Commodities: physical commodities and commodity derivatives* including exotic derivatives (e.g. weather derivatives); and
- Structured products (e.g. equity linked notes); and
- Digital decentralized cryptographic currencies (e.g. Bitcoin (BTC) or Etherium (ETH)).

Traded products confer 'rights' or 'obligations'; either between an investor and the issuer or between parties engaged in the trading of the instruments. Traded product instruments can be bought sold, borrowed or lent; as such they facilitate the transfer of property or assets and usually represent an intrinsic value which may be attractive to money launderers.

Traded products can be bought or sold either on an exchange ("exchange traded products") or between parties 'over-the- counter' (OTC).

Some traded products or instruments such as equities are issued in a 'primary' market and are traded in a 'secondary' market allowing investors in the primary market to realise their investment. Other traded products are created to enable investors to manage assets and liabilities exchange risks and exposure to particular assets commodities or securities.

Exchange-traded products

Exchange-traded products are financial products that are traded on exchanges which have standardised terms (e.g. amounts delivery dates and terms) and settlement procedures and transparent pricing. Firms may deal in exchange-traded products as principal or as agent for their customers. In the financial and commodity derivatives markets firms will typically deal as principal and on certain exchanges may only do so when dealing as a clearing member in relation to their customers' transactions. In the securities markets firms can deal as either principal (for their own account) or as agent for the firms' underlying customers.

OTC products

OTC products are bilateral agreements between two parties or multilateral depending on the settlement process that are not traded or executed on an exchange. The terms of the agreement are tailored to meet the needs of the parties* i.e. there are not necessarily standardised terms contract sizes or delivery dates. Where firms deal OTC they usually deal

as principal. Some OTC dealing is facilitated by securities companies and while settlement is normally effected directly between the parties, it is becoming increasingly common for exchanges and clearing houses to provide OTC clearing facilities.

Wholesale market sub-sectors

The products set out above are, largely, securities focused, but equally apply across the wholesale markets. The following sections look at particular products associated with other sub-sectors within the wholesale markets.

Foreign exchange

To the extent that firms dealing in foreign exchange (FX) in the wholesale market tend to be regulated financial institutions and large corporates, the money laundering risk may be viewed as generally lower. However, this risk may be increased by the nature of the customer, or where, for example:

- high risk clients (including PEPs) undertake speculative trading; and/or
- requests are made for payments to be made to third parties: for example, customers, particularly corporates, that need to make FX payments to suppliers and overseas affiliates.

FX (as well as many other traded products) is commonly traded on electronic trading systems. Such systems may be set up by securities companies or independent providers. When a firm executes a transaction on these systems the counterparty's identity is not usually known until the transaction is executed. The counterparty could be any one of the members who have signed up to the system. Firms should examine the admission policy of the platform before signing up to the system to ensure, that the platform only admits regulated financial institutions as members, or that the rules of the electronic trading system mean that all members are subject to satisfactory AML checks.

Financial derivatives

Financial products are utilised for a wide range of reasons, and market participants can be located anywhere within the world; firms will need to consider these issues when developing an appropriate risk-based approach. The nature, volume and frequency of trading, and whether these make sense in the context of the customer's and firm's corporate and financial status, will be key relevant factors that a firm will need to consider when developing an appropriate approach.

Structured products

Generally speaking, structured products are financial instruments specifically constructed to suit the needs of a particular customer or a group of customers. They are generally more complex than securities and are traded predominantly OTC, although some structured notes are also listed on exchanges (for example, the Luxembourg or Irish Stock Exchanges).

Transactions are normally undertaken on a principal basis between the provider (normally a financial institution) and the customer. Some structured products are also sold through banks and third party distributors.

Because of the sometimes complex pricing structures of the products they may generally be more difficult to value than cash securities. The lack of transparency may make it easier for money launderers for example to disguise the true value of their investments.

The complexity of the structure can also obscure the actual cash flows in the transaction enabling customers to carry out circular transactions.

The cash movements associated with structured products may present an increased money laundering risk although this risk may be mitigated by the nature and status of the customer and the depth of the relationship the customer has with the firm. For example if the use of structured products is part of a wider business relationship and is compatible with other activity between the firm and the customer the risk may be reduced. Mentioned above risk increases if the counterparties are using cryptocurrencies, not cash

Money laundering risks in wholesale market

Traded products are usually traded on regulated markets or between regulated parties or with regulated parties involved acting as agent or principal.

However the characteristics of products that facilitate the rapid and sometimes opaque transfer of ownership the ability to change the nature of an asset and market mechanisms that potentially extend the audit trail together with a diverse international customer base have specific money laundering risks that need to be addressed and managed appropriately.

One of the most significant risks associated with the wholesale markets and traded products is where a transaction involves payment in cash and/or third party payments.

Firms dealing in traded products in the wholesale markets are not as likely to be used in the placement stage of money laundering as for example deposit takers. That said given the global flows of funds in the wholesale financial markets it is important to recognise that although customers may remit funds from credit institutions a firm could still be targeted with respect to the layering and integration stages of money laundering. Traded products might for example be used as a means of changing assets rapidly into different form possibly using multiple securities companies to disguise total wealth and ultimate origin of the funds or assets or as savings and investment vehicles for money launderers and other criminals.

Firms dealing in traded products in the wholesale markets do not generally accept cash deposits or provide personal accounts that facilitate money transmission and/or third party funding that is not related to specific underlying investment transactions. In the money markets however customers may request payments to third parties (e.g. FX payments to suppliers). There may also be third party funding of the transactions in the commodities markets. Also where a bank is lending funds to a customer to purchase a physical commodity and the customer hedges the risks associated with the transaction in the derivatives market through a securities company* the bank may guarantee the payment of margin to that securities company; this results in a flow of money between the securities company and bank on the customer’s behalf.

The extent to which certain products are subject to margin or option premium payment arrangements will affect the level of risk. The nature and form of any margin will need to be taken into account by the firm when identifying the customer and determining appropriate payment procedures.

OTC and exchange-based trading can also present very different money laundering risk profiles. Most exchanges are regulated transparent and cleared by a central

counterparty and thus can largely be seen as carrying a lower generic money laundering risk. OTC business may generally be less well regulated and it is not possible to make the same generalisations concerning the money laundering risk as with exchange-traded products. When dealing in the OTC markets firms will therefore need to take a more considered and undertake more detailed assessment.

For example, regular exchanges often impose specific requirements on position transfers which have the effect of reducing the level of money laundering risk. Regular exchanges also monitor prices of exchange traded securities and will frequently investigate pricing anomalies. These procedures will not apply in the OTC markets, where firms will need to consider the approach they would adopt in relation to any such requests in respect of customers dealing OTC.

The wholesale securities market includes private equity, corporate finance, wholesale markets, name passing securities companies in inter-professional markets and unregulated funds. The retail securities market includes wealth management, financial advisers, non-life providers of investment fund products, discretionary and advisory investment management and execution-only securities companies. It is wise to remember that many cryptographic tokens represent the rights aforesaid, so our firm notes that we shall consider transactions of digital assets, representing wholesale market securities.

Retail Securities Markets

Wealth management

Overview of wealth management

Wealth management is the provision of banking and investment services in a closely managed relationship to high net worth clients who may be based in another country or may regularly travel between a number of countries. Such services will include bespoke product features tailored to a client's particular needs and may be provided from a wide range of facilities available to the client including:

- current account banking high value transactions
- use of sophisticated products
- non-standard investment solutions
- business conducted across different jurisdictions
- off-shore and overseas companies, trusts or personal investment vehicles

Multiple and complex accounts — Clients often have many accounts in more than one jurisdiction, either within the same firm or group, or with different firms.

Cultures of confidentiality — Wealth management clients often seek reassurance that their need for confidential business will be conducted discreetly.

Concealment — The misuse of services such as offshore trusts and the availability of structures such as shell companies helps to maintain an element of secrecy about beneficial ownership of funds.

Countries with statutory banking secrecy — There is a culture of secrecy in certain jurisdictions, supported by local legislation, in which wealth management is available.

Movement of funds — The transmission of funds and other assets by private clients often involve high value transactions, requiring rapid transfers to be made across accounts in different countries and regions of the world.

The use of concentration accounts — i.e. multi-client pooled/omnibus type accounts - used to collect together funds from a variety of sources for onward transmission is seen as a potential major risk.

Credit — The extension of credit to clients who use their assets as collateral also poses a money laundering risk unless the lender is satisfied that the origin and source of the underlying asset is legitimate.

Commercial activity conducted through a personal account so as to deceive the banker.

Secured loans

Secured loans, where collateral is held in one jurisdiction and the loan is made from another, are common in wealth management. Such arrangements serve a legitimate business function and make possible certain transactions which may otherwise be unacceptable due to credit risk. Collateralised loans raise different legal issues depending on the jurisdiction of the loan. Foremost among these issues are the propriety and implications of guarantees from third parties (whose identity may not always be revealed) and other undisclosed security arrangements. Our firm considers to pay close attention to transactions with such cryptographic assets, that represent any of, but not limited to, rights and obligations aforesaid.

4. Preventive Measures

Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.

Financial institutions should be required to undertake customer due diligence (CDD) measures when:

(i) establishing business relations;

(ii) carrying out occasional transactions (i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;

(iii) there is a suspicion of money laundering or terrorist financing; or

(iv) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data. The principle that financial institutions should conduct CDD should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or enforceable means. The CDD measures to be taken are as follows:

(a) dentifying the customer and verifying that customer’s identity using reliable, independent source documents, data or information.

(b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.
(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution’s knowledge of the customer, their business and risk profile,

including, where necessary, the source of funds.

Where the Company is unable to comply with the applicable requirements under paragraphs (a) to (d) above (subject to appropriate modification of the extent of the measures on a risk-based approach), it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer. These requirements should apply to all new customers, although financial institutions should also apply this recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

The Company should be required to maintain, for at least seven years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

The Company should be required to keep all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licences or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least seven years after the business relationship is ended, or after the date of the occasional transaction. Financial institutions should be required by law to maintain records on transactions and information obtained through the CDD measures. The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.

5. Customer Identification Program

We have established, documented and maintained a written Client Identification Program (CIP). We will collect certain client identification information from each client who uses QFS tokens and/or who will create an account on the stock exchange web-site to verify the identity of each client.

a. Required Customer Information

Prior to approving our services, The Company will collect the following information for all customers, if applicable, for any person, entity or organization:

(1) the name;

(2) an address, which will be a residential or business street address (for an individual).

b. Customers Who Refuse to Provide Information

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our firm will not offer our services and, after considering the risks involved, consider closing any business with the client. In either case, our AML Compliance Person will be notified so that we can determine whether we should report the situation to the regulatory body.

c. Verifying Information

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. CO 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 collected by us. We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. We may also use non-documentary means, if we are still uncertain about whether we know the true identity of the customer. In verifying the information, we will consider whether the identifying information that we receive, such as the customer's name, street address, zip code, telephone number (if provided), date of birth and Social Security number, allow us to determine that we have a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

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

- For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- For a person other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument.

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

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

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

We will use non-documentary methods of verification when:

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

(2) the firm is unfamiliar with the documents the customer presents for identification verification;

(3) the customer and firm do not have face-to-face contact; and

(4) 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.

d. Recordkeeping

Quifas Inc. follows established bookkeeping and documentation standards.

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 made about verification of the customer's identity for seven years after the record is made.

e. Comparison with Government-Provided Lists of Terrorists

At such time as we receive notice that a federal government agency has issued a list of known or suspected terrorists and identified the list as a list for CIP purposes, we will, within a reasonable period of time after entering into an agreement (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 directives issued in connection with such lists.

f. Notice to Customers

We will provide notice to customers that the firm is requesting information from them to verify their identities, as required by law. We will use the following method to provide notice to customers: Email, Phone call or certified mail.

g. Reliance on another Financial Institution for Identity Verification

We may, under the following circumstances, rely on the performance by another financial institution (including an affiliate) of some or all of the elements of our CIP with respect to any customer that is entering into an agreement or similar business relationship with the other financial institution to provide or engage in services, dealings or other financial transactions:

- when such reliance is reasonable under the circumstances;
- when the other financial institution is subject to a rule implementing the anti-money laundering compliance program requirements, and is regulated by a federal functional regulator; and
- when the other financial institution has entered into a contract with our firm requiring it to certify annually to us that it has implemented its anti-money laundering program and that it will perform (or its agent will perform) specified requirements of the customer identification program.

6. High Risk Customer Due Diligence

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

- the source of fund;
- the beneficial owners information;
- the customer’s (or beneficial owner’s) occupation or type of business;
- financial statements;
- banking references;
- domicile (where the customer’s business is organized);
- description of customer’s primary trade area and whether international transactions are expected to be routine;
- description of the business operations and anticipated volume of trading.

We will also ensure that the customer information remains accurate by following the established procedures.

7. Monitoring Clients 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: CO will be responsible for this monitoring, will review any activity that our monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

We will conduct the following reviews of activity that our monitoring system detects: Complete Account Review. We will document our monitoring and reviews as follows: according to AML Compliance. The AML Compliance Person or his or her designee will conduct an appropriate investigation and review relevant information from internal or third-party sources before a STR is filed.

a. Emergency Notification to Law Enforcement by Telephone

In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, we will immediately call an appropriate law enforcement authority. If we notify the appropriate law enforcement authority of any such activity, we must still file a timely STR. Although we are not required to, in cases where we have filed a STR that may require immediate attention of the regulatory body, we may contact it.

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

Activity Inconsistent With Business

- 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.

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. 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 STR.

8. Suspicious Transactions and BSA Reporting

Filing a STR

TEXT EXAMPLE: We will file STR with the regulatory body for any transactions (including transfers) conducted or attempted by, at or through our firm involving $15,000 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 of the existing requirements;

(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 STR 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 will report suspicious transactions by completing a STR, and we will collect and maintain supporting documentation. We will file a STR no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a STR. If no suspect is identified on the date of initial detection, we may delay filing the STR for an additional 30 calendar days pending identification of a suspect, but in no case will the reporting be delayed more than 60 calendar days after the date of initial detection. The phrase "initial detection" does not mean the moment a transaction is highlighted for review. A

review must be initiated promptly upon identification of unusual activity that warrants investigation.

We will retain copies of any STR filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the STR. We will identify and maintain supporting documentation and make such information available to any appropriate law enforcement agencies and regulatory bodies.

9. AML Recordkeeping

a. Responsibility for Required AML Records and STR Filing

Our AML Compliance Person and his or her designee will be responsible for ensuring that AML records are maintained properly and that STR is filed as required.

b. SAR-SF Maintenance and Confidentiality

We will hold STR and any supporting documentation confidential. We will not inform anyone outside of appropriate law enforcement or regulatory agencies about a STR.

10. 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 CO. Such reports will be confidential, and the employee will suffer no retaliation for making them.

11. Additional Risk Areas

The firm has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above.

12. 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.

N.B. This Compliance Manual is to be strictly adhered to by all Employees. Non-compliance with this Compliance Manual by any Employee shall result in disciplinary actions. There are no exceptions to this Compliance Manual without the prior written approval of the Compliance Officer. Any questions, comments or concerns regarding the Firm's anti-money laundering policies, procedures and controls should be directed to the Compliance Officer.