Anti-Money Laundering and Counter Terrorism Financing (AML&CTF) Program:

Compliance and Supervisory Procedures

UPDATED AS OF NOVEMBER 26, 2018

## Firm Policy

It is the policy of 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 (AML&CTF) and its implementing regulations.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

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

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Our AML policies, procedures and internal controls are designed to ensure compliance with all of AML&CTF Act No. 13 of 2014 and the VFIU. If any transaction or proposed transaction is deemed to be a suspicious transaction, we will submit a report to the VFIU.

Outlined are our principles within the company in regards to our AML & CTF Policies:

* We are opposed to the crimes of money laundering and terrorism financing and do not tolerate the use of our products and services for either of these purposes.
	+ - We are committed to playing our role in the fight against money laundering and terrorism financing in the Vanuatu.
		- We will comply with the letter and the spirit of the laws and regulations of the Vanuatu that relate to AML & CTF.
		- We will provide our products and services only for legitimate purposes to persons whose identities we have been able to reasonably ascertain.
		- We will avoid relationships with those that we reasonably assess as representing too high a risk of money laundering or terrorism financing.
		- We will help our staff manage the issues that might arise for them when dealing with people they know, including kin.
		- Our owners, management and staff will be treated in the same way as all other Applicants when they apply to use our services.
		- We report any activity that we detect which we regard as suspicious to our VFIU.
		- Our staff will receive the AML & CTF training they need to understand their obligations under the law and to perform in their roles.
		- We will monitor our customers, their transactions, and our people, consistent with the level of money laundering and terrorism financing risk they represent.
		- We will comply with the requirement under Section 9 of the AML & CTF Act to register with the FIU and inform them of any material changes that may occur within our business at any time.
		- Our office will adhere to the requirements under Section 34 of the AML & CTF Act to report to the FIU on the appointment of or update on any changes regarding our Compliance Officer.
		- We are aware that our owners, management and staff are subject to a fit and proper screening by FIU and could be removed pursuant to Section 48 as a disqualified person within the meaning of section 49 of the AML & CTF Act by FIU

Our AML & CTF Program and policies are made up of the contents of this document. Our activities to ensure our compliance are as follows:

* Accept Applications for transactions
* Monitor the transactions for unusual activity that may need further investigation
* Identify events that require us to take further action
* Report certain matters to the VFIU
* Keep records of all of our actions

In regards to our disciplinary actions that will be used upon misconduct, all staff will understand that they will face disciplinary action, and possible dismissal, under any circumstance where they fail to follow the AML & CTF procedures and requirements in this document. We will dismiss any person facilitating money laundering and terrorism financing or is involved in any capacity with money laundering or terrorism financing. Law Enforcement will receive are full cooperation in the persecution of such matter against our staff.

We understand that sometimes our customers or transactions involve people we know well. Our staffs are still expected to follow the procedures within this document. Staff should go to the Compliance officer if they are experiencing difficulties within this area.

## 2. AML Compliance Person Designation and Duties

The firm has designated Christian Kang as its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the firm’s AML program. Christian Kang has a working knowledge of the AML & CTF Act 13 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, and assessing risk on all our clients regularly based on the information collected. 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 (STRs) are filed with the Vanuatu Financial Intelligence Unit (VFIU) when appropriate. The AML Compliance Person is vested with full responsibility and authority to enforce the firm’s AML program.

The firm will provide VFSC with contact information for the AML Compliance Person through the VFSC Contact System including: (1) name; (2) title; (3) mailing address; (4) email address; (5) telephone number; and (6) facsimile (if any). The firm will promptly notify VFSC of any change in this information and will review, and if necessary update, this information within 17 business days after the end of each calendar year. The annual review of information will be conducted by Christian Kang 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, Christian Kang will update the information promptly, but in any event not later than 30 days following the change.

It is essential that all staff know their duties within our organization and understand their duties in order to comply with the requirements outlined in this document. They are as follows:

## All staff and owners

* + - Are expected to comply fully with all of the procedures in this manual.
		- Must receive regular AML & CTF training, including training about detection and reporting of unusual and suspicious activity by customers.
		- Are expected to report any unusual or suspicious activity detected to the CO.
		- Are expected to understand the law regarding tipping-off and comply with our anti-tipping-off procedures.
		- Are expected to cooperate fully with the CO and the VFIU in the investigation of any possible breaches of the laws and regulations of the Vanuatu that relate to AML & CTF.

## Owners

* + - Our owners set the tone for our business regarding its commitment to AML & CTF.
		- Our owners must ensure that this manual meets the requirements of the laws and regulations of the Vanuatu that relate to AML & CTF and must oversee and monitor compliance with this manual.

## Compliance Officer (CO)

The CO is a senior staff member reporting to Weevelop and is responsible for:

* + - Creating and keeping this manual current;
		- Monitoring the compliance by our business with the requirements of the laws and regulations of the Vanuatu that relate to AML & CTF;
		- Monitoring transactions undertaken for Customers;
		- Identification and management of money laundering risk using our services;
		- Providing leadership and training on AML & CTF issues to our staff, including new staff;
		- Acting as the liaison point with the VFIU;
		- Investigating unusual matters and reporting those that are suspicious to our VFIU;
		- Reporting all other matters that must be reported to the VFIU;
		- Ensuring that our staff know what their responsibilities are;
		- Monitoring employees in the course of performance of their duties;
		- Ensuring that our staff are aware of the requirements of this manual and of the AML & CTF laws and regulations that apply to our business;
		- Helping our staff where they face problems associated with Customers who they know well or who are kin;
		- Overseeing corrective actions where gaps are identified in our operations with the procedures in this manual;
		- Reviewing this manual periodically for its adequacy;
		- Arranging for periodic independent review of this man

## Supervisors

Our supervisors are the most senior person on duty during our hours of operation and they are responsible for:

* + - Following the processes and procedures in this manual and being seen by the other staff to follow them;
		- Ensuring that the staff they supervise follow the processes and procedures in this manual;
		- Promoting required AML & CTF behavior by coaching, teaching, leading and encouraging other staff.
		- Helping our staff where they face problems associated with Customers who they know well or who are kin;
		- Allowing staff to attend AML & CTF training and awareness sessions;
		- Cooperating fully with the CO regarding any matters associated with compliance with the AML & CTF laws and regulations of the Vanuatu.

## Counter staff

Our counter staffs deal with our customers and accept instructions for transactions and they are responsible for:

* + - Following the identification and verification procedures in this manual;
		- Completing transactions in accordance with the procedures in this manual and in other procedures for our business;
		- Reporting any breaches of identification and verification procedures to the CO;
		- Reporting any signs of unusual, suspicious or illegal activity by customers to the CO;
		- Attending all AML & CTF training sessions that are scheduled.

## Operations

Our operations staff process transactions and perform other activities associated with our business and they are responsible for:

* + - Following the procedures in this manual;
		- Completing transactions in accordance with the procedures in this manual and in other procedures for our business;
		- Reporting any breaches of identification and verification procedures to the CO;

## Training and Trainees

The CO will ensure that all new staff members or employees are trained and made aware of this manual before they commence handling customers and transactions. He will also ensure all current staff attend AML/CFT training at least annually. Records will be kept for 6 years from the date that training was provided:

* + - Who was trained
		- What material they were trained with
		- The attendance logs by attendees
		- The date they were trained

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

### a. VFIU Requests

We will respond to a Vanuatu Financial Intelligence Unit (VFIU) request 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. We will designate through the VFSC Contact System one or more persons to be the point of contact (POC) for Requests and will promptly update the POC information following any change in such information. (See also Section 2 above regarding updating of contact information for the AML Compliance Person.) Unless otherwise stated in the Request or specified by VFIU, we are required to search those documents outlined in VFIU’s FAQ. If we find a match, Christian Kang will report it to VFIU within 14 days or within the time requested by VFIU in the request. If the search parameters differ from those mentioned above (for example, if VFIU limits the search to a geographic location), Christian Kang will structure our search accordingly.

If Christian Kang searches our records and does not find a matching account or transaction, then Christian Kang will not reply to the Request. We will maintain documentation that we have performed the required search by noting all searches done in reaction to the Request and sending said information regarding our results in relation to the Request.

We will not disclose the fact that VFIU has requested or obtained information from us, except to the extent necessary to comply with the information request. Christian Kang will review, maintain and implement procedures to protect the security and confidentiality of requests from VFIU similar to those procedures established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act with regard to the protection of customers’ nonpublic information.

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

Unless otherwise stated in the 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.

1. **National Security Letters**

We understand that the receipt of a 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 the FBI or other federal government authority has sought or obtained access to any of our records. To maintain the confidentiality of any NSL we receive, we will process and maintain the NSL by keeping it a need-to-know basis for all and any NSL we receive. Through this method, we will make sure that only our most trusted individuals at the company know that such a letter was received. If we file a STR after receiving an NSL, the STR will not contain any reference to the receipt or existence of the NSL. The STR will only contain detailed information about the facts and circumstances of the detected suspicious activity.

1. **Grand Jury Subpoenas**

We understand that the receipt of a grand jury subpoena concerning a customer does not in itself require that we file a Suspicious Transaction Report (STR). When we receive a grand jury 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 STR in accordance with the STR filing requirements. We understand that none of our officers, employees or agents may directly or indirectly disclose to the person who is the subject of the subpoena its existence, its contents or the information we used to respond to it. If we file a STR after receiving a grand jury subpoena, the STR will not contain any reference to the receipt or existence of the subpoena. The STR will only contain detailed information about the facts and circumstances of the detected suspicious activity.

### d. Voluntary Information Sharing With Other Financial Institutions

We will share information with other financial institutions regarding individuals, entities, organizations and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering. Christian Kang will ensure that the firm files with VFIU an initial notice before any sharing occurs and annual notices thereafter. We will use the notice form found at VFIU’s website. Before we share information with another financial institution, we will take reasonable steps to verify that the other financial institution has submitted the requisite notice to VFIU, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that VFIU will make available. We understand that this requirement applies even to financial institutions with which we are affiliated, and that we 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 STRs by Broker-Dealers and Other Financial Institutions**

We will file joint STRs in the following circumstances, according to our personal procedures. 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 STR.

We will share information about particular suspicious transactions with our clearing broker for purposes of determining whether we and our clearing broker will file jointly a STR. In cases in which we file a joint STR 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 STR.

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

### f. Sharing STRs With Parent Companies

Because we are a subsidiary, we may share STRs with Zenith Bridge. Before we share STRs with Zenith Bridge, we will have in place written confidentiality agreements or written arrangements that Zenith Bridge protect the confidentiality of the STRs through appropriate internal controls.

The confidentiality agreement will state that the recipient foreign parent entity (or entities) may not disclose further any STR, or the fact that such report has been filed. The agreement will allow for the foreign parent entity (or entities) to disclose without permission underlying information (that is, information about the customers and transaction(s) reported) that forms the basis for the STR and that does not explicitly reveal that a STR was filed and that is not otherwise subject to disclosure restrictions.

## Checking the Office of Foreign Assets Control Listings

Before opening an account, and on an ongoing basis, Christian Kang will check to ensure that a customer does not appear on the SDN list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by 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. Christian Kang will also review existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated and he 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 OFAC, we will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC within 10 days. We will also call the OFAC Hotline immediately.

Our review will include customer accounts, transactions involving customers (including activity that passes through the firm such as wires) and the review of customer transactions that involve physical security certificates or application-based investments (e.g., mutual funds).

## 5. Customer Identification Program

In addition to the information we must collect, we have established, documented and maintained a written Customer Identification Program (CIP). 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.

**a. Required Customer Information**

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

(1) their full name;

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

(3) a permanent 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);

(4) Occupation;

(5) Purpose or Intent in pursuing this business relationship with the company.

(6) Authorization of anything person purporting to act for or on behalf of the customer and the identity of the person.

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.
All Applicants must sign their application form with their usual signature and where an automated sales receipt is used, they must also sign this receipt.

All Applicants who are Legal persons as customer and for a Legal arrangement as customer the reporting entity would collect the customer information set out in Table A of schedule 2(as amended) or at a minimum as per the list set out in Clause 3 Prescribed Identification Process of the Regulations Order No 153 of 2015 part (b)(ii) and (c)(ii) respectively.

The CO is expected to have a full understanding of the purpose and intended nature of the business relationship with the reporting entity and the customer’s beneficial ownership and control structure.

### b. Customers Who Refuse to Provide Information

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our firm will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, our AML Compliance Person will be notified so that we can determine whether we should report the situation to VFIU on a STR. The Applicant will not be notified in any capacity of the reporting of the matter to the CO or what decision is to be made about reporting the matter to the VFIU. Our Staff that fail to comply with this procedure understand that this may be a criminal offense.

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

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

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

* For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar 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 source.
* 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.

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

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

**d. Lack of Verification**

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

Staff that may know applicants personally or may have a kin relationship with the Applicant, must still always require those Applicants to successfully complete the identification and verification procedure, including production of current and valid identification documents. As such, Applicants who are well known due to prominent public standing are still required to successfully complete the identification and verification procedures. Staff experiencing difficulties with this part of the procedure should contact the CO.

**e. 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. If only category B documents (documents with no photographic identification) were provided/accepted for the verification process, our staff will make a note as to the reason why these documents were accepted.

As there are problems with identity documentation in the Vanuatu the CO keeps an Exception Register of persons who have difficulty in easily producing these documents regularly or who are unable to attend in person because of their health, remote location or age. Counter staff may use this Exception Register to establish verification of identity for these Applicants.

The CO will keep the following information in the Exception Register:

* Full details of the Applicant’s identification information;
* A record of the verification documents used to establish identity;
* A record of the reasons why producing this information for each application is difficult.

The CO will review Applicants in the Exception Register every three years to confirm that their identification information is current.

The Exception Register cannot be used for higher risk Applicants or for transactions in excess of VT400, 000.

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

### g. 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 use the following method to provide notice to customers: Email Customers in which they have a set time period of 72 hours to respond with the required information to verify their identities. If there is no response, we will contact the customer by phone if provided. If no such record exists, we will be unable to open an account with the customer.

**Important Information About Procedures for Opening a New Account**

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

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

### h. Reliance on Another Financial Institution for Identity Verification

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 opening an account or has established an account or similar business relationship with the other financial institution to provide or engage in services, dealings or other financial transactions:

* when such reliance is reasonable under the circumstances;
* when the other financial institution is subject to a rule implementing the anti-money laundering compliance program requirements of 31 U.S.C. § 5318(h), 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. Customer Due Diligence Rule**

In addition to the information collected, we have established, documented and maintained written policies and procedures reasonably designed to identify and verify beneficial owners of legal entity customers and comply with other aspects of the Customer Due Diligence (CDD) Rule. We will collect certain minimum CDD information from beneficial owners of legal entity customers. We will understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile. We will conduct ongoing monitoring to identify and report suspicious transactions, and, on a risk basis, maintain and update customer information.

An Applicant who has satisfied the identification process (and verification process) and has established a business relationship with us is now known as a “Customer”.

Transaction Monitoring Process as per Clause 8 (1) (a) of the Regulations Order 122 of 2014 whereby transactions or attempted transactions are monitored so to identify any suspicious, complex, unusual, and have no apparent visible economic or lawful- purpose transaction. The transaction monitoring system will search transactions that are conflicting with the information held about the business relationship with the reporting entity.

Customer Monitoring Process as per clause 8 (1)(b) of the Regulations Order 122 of 2014 where the relationship of the business with its customer is monitored to ensure that the customers activities being conducted are consistent with the business knowledge of the customer, the customer’s business, source of funds and risk profile.

* 1. **Identification and Verification of Beneficial Owners**

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

(1) the name;

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

(3) an address, which will be a residential or business street address (for an individual), or 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); and

(4) an identification number, which will be a Social Security number (for U.S. persons), 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 non-U.S. persons).

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.

Where an Applicant does not attend our office in person but sends someone to present the application and perform the transaction for them then the steps below must be completed. The reasons this might occur include:

* + - * Poor mental or physical health;
			* Geographical remoteness; or
			* Advanced age.

The person representing the Applicant needs to provide written authority of the basis on which they represent the Applicant. This authority must be an original document, not a copy. Usually it will be a letter written to our business confirming permission to perform the transaction in the application and signed by the Applicant.

The application must be accompanied by certified copies of the Applicant’s identification documents. The person certifying the documents must be a suitable person such as a lawyer, accountant, commissioner of oath or manager of a Vanuatu’ domestic bank. The certified document must include a statement that the certifier has compared this copy document with the original and certifies that it is a true copy and provided details of the certifier’s name, position and contact address and telephone number.

For all transactions over VT1 million or its equivalent in foreign currency, the counter staff will call the certifier and confirm that they did certify the identification documents.

For all transactions over VT10 million or its equivalent in foreign currency, the counter staff will try to contact the Customer and verify the transaction. If the Customer cannot be contacted then a letter will be sent confirming the transaction to the Customer’s address.

Where there are repeated transactions by an Customer who does not attend our office then unless they are physically unable to attend the matter should be reported to the CO who will decide whether to permanently refuse such transactions unless the Customer attends in person with their identification documents and subjects themselves to our identification and verification procedure.

Persons doing transactions for the benefit of a third party in their own name will be asked that this transaction is being done by them for their own benefit and using their own money. If a Customer says that the transaction is for another person or uses money from another person then the application must be made by that other person and they much be successful in completing our identification and verification procedure.

**Special Transaction Controls**

We have the following transaction types:

* + - * Purchase of money orders
			* Purchase of travellers’cheques
			* Cashing money orders
			* Cashing travellers’cheques
			* Sending money to another person in the Vanuatu
			* Receiving money for a person from someone else in the Vanuatu
			* Sending money to another person overseas
			* Receiving money for a person from someone else overseas
			* Exchanging VT for foreign currency
			* Exchanging foreign currency for VT
			* Exchanging one foreign currency for another foreign currency.

## Application forms are different for different transactions

Counter staff must ensure that the correct application form is used for each transaction. Each form has been designed to get the right information from the Applicant.

All Applicants must complete all the required information fields on the application form which applies to their transaction.

Staff must not accept incomplete application forms.

Where an Applicant insists that they cannot provide all the information requested, or the information provided does not make sense then their application should be referred to the CO for her approval.

The CO will decide whether the absence of certain information or the nature of the information is such that the transaction can still proceed, alternatively whether it should be refused and the application reported to the VFIU.

If the application is refused by the CO then the Applicant must not be informed about what decision was made about reporting the matter to the VFIU. Failure to comply with this procedure may be a criminal offence.

Counter staff and Operations staff are responsible for checking that the information provided on each application makes sense. They cannot ignore other information they may know about the Applicant or the transaction just because it is not on the application form.

## Compliance with these procedures

No transaction may be completed unless all the information required has been provided. However the CO does have power to over-ride this in limited circumstances.

Counter staff repeatedly accepting transactions without all the required information will be subject to disciplinary action and potential dismissal.

Counter staff must be careful to insist on provision of all the required information even though they or someone else in our office may have a kin relationship with the Applicant.

Counter staff should go to the CO if they are experiencing difficulties with this part of our procedures.

## Enhanced Identification and Verification process

Staff who become aware of the status of an applicant or customer that he/she occupy and is defined as someone listed under 9.1 or the beneficiary of a transaction as someone listed under 9.1, must immediately inform the CO.

Our CO must, in addition to the normal identification and verification process,

* + - * collect additional information on the applicant (volume of assets, information available through public domain)
			* collect additional information the intended nature of the business relationship
			* collect information on the source of the funds or source of wealth
			* collect information on the ultimate beneficiary
			* Obtain the senior management’s approval to commence the business relationship.
			* Request the applicant/customer to carry out the first transaction/payment to be carried out through a bank account under the customer’s name

Our CO will keep records of all his findings and the senior management decision.

* 1. **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 personally meeting customers or speaking on the phone.

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.
	1. **Conducting Ongoing Monitoring to Identify and Report Suspicious Transactions**

We will conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, maintain and update customer information, including information regarding the beneficial ownership of legal entity customers, using the customer risk profile as a baseline against which customer activity is assessed for suspicious transaction reporting. Our suspicious activity monitoring procedures are detailed within Section 11 (Monitoring Accounts for Suspicious Activity).

## 7. Correspondent Accounts for Foreign Shell Banks

### a. Detecting and Closing Correspondent Accounts of Foreign Shell

We will identify foreign bank accounts and any such account that is a correspondent account (any account that is established for a foreign bank to receive deposits from, or to make payments or other disbursements on behalf of, the foreign bank, or to handle other financial transactions related to such foreign bank) for foreign shell banks by recording customer money flow and requests for sudden changes to bank infomation. Upon finding or suspecting such accounts, firm employees will notify the AML Compliance Person, who will terminate any verified correspondent account in the United States for a foreign shell bank. We will also terminate any correspondent account that we have determined is not maintained by a foreign shell bank but is being used to provide services to such a shell bank. We will exercise cautionregarding 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.

 **b. Certifications**

We will require our foreign bank account holders to identify the owners of the foreign bank if it is not publicly traded, the name and street address of a person who resides in the United States and is authorized and has agreed to act as agent for acceptance of legal process, and an assurance that the foreign bank is not a shell bank nor is it facilitating activity of a shell bank. In lieu of this information the foreign bank may submit the Certification Regarding Correspondent Accounts For Foreign Banks provided in the AML&CTF regulations. We will re-certify when we believe that the information is no longer accurate or at least once every three years.

###  c. Recordkeeping for Correspondent Accounts for Foreign Banks

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.

### d. Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationships with Foreign Bank

When we receive a written request from a federal law enforcement officer for information identifying the non-publicly traded owners of any foreign bank for which we maintain a correspondent account in the United States and/or the name and address of a person residing in the United States who is an agent to accept service of legal process for a foreign bank’s correspondent account, we will provide that information to the requesting officer not later than seven days after receipt of the request. We will close, within 10 days, any correspondent account for a foreign bank that we learn from VFIU or the Department of Justice has failed to comply with a summons or subpoena issued by the Secretary of the Treasury or the Attorney General of the United States or has failed to contest such a summons or subpoena. We will scrutinize any correspondent 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 correspondent accounts.

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

## a. Due Diligence for Correspondent Accounts of Foreign Financial Institutions

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 risk 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 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**

Staff must immediately inform our CO of any and all transactions conducted by a customer listed under 9.3 or 9.4.

Our CO must, in addition to information collected earlier:

* + - * Collect satisfactory information on the ultimate beneficiary of the transaction and on whose behalf the transaction was conducted
			* Collect satisfactory information on the source of the fund in relation to the transaction
			* Collect satisfactory information on the intended reason for the transaction
			* Obtain the senior management approval for the transaction

Our CO must conduct strictly 3-monthly monitoring on our relationship with persons posing some level of AML&CTF risk and regularly update our information on such person’s identification and verification including id documents (data).

**Correspondent Banking**

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 STR, close the correspondent account and/or take other appropriate action.

## 9. The Risk

**Applicants and Customers**

Applicants and applications received must be assessed on the level of AML&CTF risks they may impose on our entity and all transactions over a 400,000vt threshold conducted by said customers requires on-going CDD.

## Introduced Applicants/Customer

Applicants or customers who are introduced to the business by our intermediaries or third party introducers and did not appear in person in the customer acceptance process must be subject to the requirements under section 8.

## Applicants/Customers wishing to use high risk products/services or use high risk delivery method

Applicants or customers who are deemed as ‘low risk’ but wish to engage our services/products which we deemed as ‘high risk’ or delivery methods which are deemed as ‘high risk’ are subject to the requirements listed under section 8.4 and 8.5.

## Customers with adverse financial report against them

Customers with adverse reports against them are subject to the requirements listed under section 8.

## Customers representing or are legal entities/arrangements

Customers representing or are legal entities/arrangement are subject to the requirements listed under section 8.

## Product/Service Risk

Large Principal Money Transfers (LPMT) (Money Remitters) >VT 30,000 ***(illustrative example)***

All applications for LPMTs must be made in person and contain:

* + - * + The amount of the transaction
				+ The currency
				+ Source of the funds
				+ Description of the origin of the funds
				+ Purpose of the transaction
				+ Sender’s full name
				+ Sender’s occupation
				+ Sender’s means of identification and details of the identification document
				+ Receiver’s full name
				+ Details of the relationship between Sender and Receiver
				+ Supporting documents such as invoices, purchase orders, contracts.

Applications for LPMTs are not accepted from people under the age of 18 years.

Once the application has been made the details cannot be changed.

The receiver must provide valid identification before the money can be paid.

All refused and incomplete applications should be reported to the CO who in turn should report them to the VFIU.

All applications for LPMTs must be approved by the CO who may also need to obtain the consent of the franchisor.

## High volume transactions

Customers conducting high volume transactions (i.e. whether the amount of the transaction is significant above the in-house threshold or conducting several transactions which the sum total to an amount above the in-house threshold) are subject to the requirements listed under section 8.4 and 8.5.

## Politically Exposed Person

We consider the following persons are persons who may pose some level of AML&CTF risk to the business:

* + - * Person who is or has been entrusted with prominent public functions (e.g. Head of State and Prime Minister)
			* Serving Government Minister
			* Serving Member of Parliament
			* Serving senior officials of political party
			* Serving senior Military officials
			* Serving senior judicial officials
			* Serving senior executive members of state owned corporation
			* Serving senior executive members of international organisation
			* Person who has been convicted of a criminal financial offence not less than 2 years
			* Director of a legal person or legal arrangement who has been convicted of a criminal financial offence not less than 3 years

## High Risk Business Relationship

We must categorize applicants with appropriate risk level.

High risk relationships, we must examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions and unusual pattern of transaction which have no apparent economic or lawful purpose.

High Risk Customer must be subject to the requirement listed under section 8.5 of the Procedures Manual

## Higher risk countries

The following countries are considered high risk countries:

* + - Iran
		- Burma/Myanmar
		- Nigeria
		- Democratic People’s Republic of Korea (DPRK)
		- Cuba
		- Bolivia
		- Ethiopia
		- Ghana
		- Indonesia
		- Kenya
		- Pakistan
		- Sao Tome & Principe
		- Sri Lanka
		- Syria
		- Tanzania
		- Thailand
		- Turkey

All applications from applicants originated or possess identification/verification documents from the high risk country must be forwarded to the CO for her and senior management’s review and approval.

If the application is approved, the CO must conduct enhanced on-going due diligence on the applicant and transactions.

The CO must report any unusual matter to the VFIU.

## Non-Resident Applicant

Non-resident applicants are subject to the requirements listed under section 8.4 and 8.5.

## Products/Service Delivery Method

**Organizational Structure**

**DECLINED BUSINESS**

We do not accept business from the following people:

* + - Prescribed Money Laundering entity
		- Prescribed terrorist organizations
		- Serving inmates
		- Minors (under the age of 16 years old)
		- Customers operating under false or misleading names that we become aware of
		- who does not produce identity or verification within prescribed timeframe

## 10. Compliance with VFIU’s Issuance of Special Measures Against Foreign Jurisdictions, Financial Institutions or International Transactions of Primary Money Laundering Concern

IfVFIU issues a final rule imposing a special measure againstone or more foreign jurisdictions or financial institutions, classes of international transactions or types of accounts deeming them to be of primary money laundering concern, we understand that we must read VFIU’s final rule and follow any prescriptions or prohibitions contained in that rule. For example, if the final rule deems a certain bank and its subsidiaries (Specified Banks) to be of primary money laundering concern, a special measure may be a prohibition from opening or maintaining a correspondent account in the United States for, or on behalf of, the Specified Banks. In that case, we will take the following steps:

(1) We will review our account records, including correspondent account records, to ensure that our accountholders and correspondent accountholders maintain no accounts directly for, or on behalf of, the Specified Banks; and

(2) We will apply due diligence procedures to our correspondent accounts that are reasonably designed to guard against indirect use of those accounts by the Specified Banks. Such due diligence may include:

• Notification to Correspondent Accountholders

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

We will transmit the notice to our correspondent accounts using the following method: Email and personal message from our platform and we shall retain documentation of such notice.

• Identification of Indirect Use

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

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

## 11. Monitoring Accounts for Suspicious Activity

We will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business. (Red flags are identified in Section 11.b. below.) Monitoring will be conducted through the following methods: careful and thorough inspection of all accounts on a regular basis. 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.

We will conduct the following reviews of activity that our monitoring system detects: activity concerning transactions of large sums or withdrawals into accounts not normally withdrawn to. We will document our monitoring and reviews in detail in relation to all suspicious activity. 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. Other contact numbers we will use are: VFIU’s Financial Institutions Hotline (especially to report transactions relating to terrorist activity). If we notify the appropriate law enforcement authority of any such activity, we must still file a timely a STR.

Although we are not required to, in cases where we have filed a STR that may require immediate attention by the VFIU, we may contact the VFIU via the VFIU STR Alert Message Line to alert the SEC about the filing. We understand that calling the VFIU STR Alert Message Line does not alleviate our obligations to file a STR or notify an appropriate law enforcement authority.

### b. 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 AML&CTF 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 accountactivity 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 the AML Compliance Person. 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.

**12. Suspicious Transactions and Reporting to the VFIU**

### a. Filing a STR

 We will file STRs with VFIU for any transactions (including deposits and transfers) conducted or attempted by, at or through our firm involving $5,000, or its equivalent in foreign currency, 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 the AML&CTF regulations;

(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. In addition, although we are not required to, we may contact that SEC in cases where a STR we have filed may require immediate attention by the SEC. See Section 11 for contact numbers. 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 STR rule, we must file a STR reporting the violation.

We may file a voluntary STR 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 STR rule. It is our policy that all STRs will be reported regularly to the Board of Directors and appropriate senior management, with a clear reminder of the need to maintain the confidentiality of the STR.

We will report suspicious transactions by completing a STR, and we will collect and maintain supporting documentation as required by the AML&CTF regulations. We will file a STR-SF 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. 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 STR requirements. 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-SF. We will identify and maintain supporting documentation and make such information available to VFIU, any other appropriate law enforcement agencies, federal or state securities regulators or SROs upon request.

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the AML&CTF regulations. We understand that anyone who is subpoenaed or required to disclose a STR or the information contained in the STR will, except where disclosure is requested by VFIU, the SEC, or another appropriate law enforcement or regulatory agency, or an SRO registered with the SEC, decline to produce the STR or to provide any information that would disclose that a STR was prepared or filed. We will notify VFIU of any such request and our response.

### b. Currency Transaction Reports

We will keep financial records of all currency transaction reports. If we detect a transaction that exceeds $10,000, or its equivalent in foreign currency,, we will file with VFIU CTRs for currency transactions that exceed $10,000, or its equivalent in foreign currency. Also, we will treat multiple transactions involving currency as a single transaction for purposes of determining whether to file a CTR if they total more than $10,000, or its equivalent in foreign currency, and are made by or on behalf of the same person during any one business day. We will use the AML&CTF E-Filing System to file the supported CTR Form.

### c. Currency and Monetary Instrument Transportation Reports

Our firm prohibits both the receipt of currency or other monetary instruments that have been transported, mailed or shipped to us from outside of the United States, and the physical transportation, mailing or shipment of currency or other monetary instruments by any means other than through the postal service or by common carrier. We will file a CMIR with the Commissioner of Customs if we discover that we have received or caused or attempted to receive from outside of the U.S. currency or other monetary instruments in an aggregate amount exceeding $10,000, or its equivalent in foreign currency, at one time (on one calendar day or, if for the purposes of evading reporting requirements, on one or more days). We will also file a CMIR if we discover that we have physically transported, mailed or shipped or caused or attempted to physically transport, mail or ship by any means other than through the postal service or by common carrier currency or other monetary instruments of more than $10,000, or its equivalent in foreign currency, at one time (on one calendar day or, if for the purpose of evading the reporting requirements, on one or more days). We will use the Form provided on VFIU’s website.

### Foreign Bank and Financial Accounts Reports

We will file a Foreign Bank and Financial Accounts Report (FBAR) for any financial accounts of more than $10,000, or its equivalent in foreign currency, that we hold, or for which we have signature or other authority over, in a foreign country. We will use the AML&CTF E-Filing System provided on VFIU’s website.

**e. Monetary Instrument Purchases**

When we issue or sell a bank check or draft, cashier's check, money order or traveler's check in the amounts of $3,000 to $10,000, or its equivalent in foreign currency, inclusive, we will maintain records of the following information:

(a) (1) If the purchaser has a deposit account with us:

(i) (A) the name of the purchaser;

 (B) the date of purchase;

(C) the type(s) of instrument(s) purchased;

(D) the serial number(s) of each of the instrument(s) purchased; and

(E) the amount in dollars of each of the instrument(s) purchased.

(ii) In addition, we must verify that the individual is a deposit accountholder or must verify the individual's identity. Verification may be either through a signature card or other file or record provided the deposit accountholder's name and address were verified previously and that information was recorded on the signature card or other file or record; or by examination of a document which is normally acceptable as a means of identification when cashing checks for nondepositors and which contains the name and address of the purchaser. If the deposit accountholder's identity has not been verified previously, we shall verify the deposit accountholder's identity by examination of a document which is normally acceptable within the community as a means of identification when cashing checks for nondepositors and which contains the name and address of the purchaser, and shall record the specific identifying information (e.g., driver’s license number and state of issuance).

(2) If the purchaser does not have a deposit account with us:

(i) (A) the name and address of the purchaser;

(B) the Social Security number of the purchaser, or if the purchaser is an alien and does not have a Social Security number, the alien identification number;

(C) the date of birth of the purchaser;

(D) the date of purchase;

(E) the type(s) of instrument(s) purchased;

(F) the serial number(s) of the instrument(s) purchased; and

(G) the amount in dollars of each of the instrument(s) purchased.

(ii) In addition, we shall verify the purchaser's name and address by examination of a document which is normally acceptable within the community as a means of identification when cashing checks for nondepositors and which contains the name and address of the purchaser, and shall record the specific identifying information (e.g., driver’s license number and state of issuance).

(b) Contemporaneous purchases of the same or different types of instruments totaling $3,000 or more shall be treated as one purchase. Multiple purchases during one business day totaling $3,000 or more shall be treated as one purchase if an individual employee, director, officer or partner of the Weevelop has knowledge that these purchases have occurred.

(c) We shall keep records required to be kept for a period of five years, and such records shall be made available to the federal and state authorities or SROs upon request at any time.

### f. Funds Transmittals of $3,000 or More Under the Travel Rule

When we are the transmittor’s financial institution in funds of $3,000 or more, we will retain either the original or a copy (e.g., microfilm, electronic record) of the transmittal order. We will also record on the transmittal order the following information: (1) the name and address of the transmittor; (2) if the payment is ordered from an account, the account number; (3) the amount of the transmittal order; (4) the execution date of the transmittal order; and (5) the identity of the recipient’s financial institution. In addition, we will include on the transmittal order as many of the following items of information as are received with the transmittal order: (1) the name and address of the recipient; (2) the account number of the recipient; (3) any other specific identifier of the recipient; and (4) any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order.

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.

## Incomplete wire transfers

If we have a wire transfer that does not contain complete originator information – the name, address and account number of the remitter then we always report these as suspicious and wait for instructions from the VFIU on how to proceed.

## Tipping off

Our staff are prohibited from discussing any unusual matter, cash transaction or international funds transfer they report to the CO with any other person within or outside our business unless they have the CO’s consent to do so.

Our CO is prohibited from discussing any report or unusual matter they investigate, or what the outcome of their investigation was with any person within or outside our business except where they need to do so to complete their investigation, or if they need advice or assistance. This includes management and owners.

Our CO will send any staff person who reports an unusual matter a reminder about the prohibition in section 38 of the AML & CTF Act on tipping off.

Our staff receives training regarding the prohibition in section 38 of the AML & CTF Act regarding tipping off.

## Requests

Our CO will provide any additional information that is requested by the FIU as per section 32 of the AML & CTF Act

In addition, our business will submit an AML & CTF Compliance Report when requested as per section 31 of the AML & CTF Act.

Our Procedures Manual would be submitted to VFIU upon request as per section 33(3) of the AML & CTF Act.

Our Risk Assessment will be conducted and submitted to the VFIU upon request as per section 35 of the AML & CTF Act.

## 13. 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 STRs are filed as required.

In addition, as part of our AML program, our firm will create and maintain STRs, CTRs, CMIRs, FBARs, and relevant documentation on customer identity and verification (See Section 5 above) and funds transmittals. We will maintain STRs and their accompanying documentation for at least five years. We will keep other documents according to existing AML&CTF and other recordkeeping requirements, including certain rules that require six-year retention periods.

### b. STR Maintenance and Confidentiality

We will hold STRs and any supporting documentation confidential. We will not inform anyone outside of VFIU, the SEC, an SRO registered with the SEC or other appropriate law enforcement or regulatory agency about a STR. We will refuse any subpoena requests for STRs or for information that would disclose that a STR has been prepared or filed and immediately notify VFIU of any such subpoena requests that we receive. See Section 11 for contact numbers. We will segregate STR filings and copies of supporting documentation from other firm books and records to avoid disclosing STR filings. Our AML Compliance Person will handle all subpoenas or other requests for STRs. We may share information with another financial institution about suspicious transactions in order to determine whether we will jointly file a STR according to the provisions of Section 3.d. In cases in which we file a joint STR for a transaction that has been handled both by us and another financial institution, both financial institutions will maintain a copy of the filed STR.

### 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, or its equivalent in foreign currency,, 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, or its equivalent in foreign currency, 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, or its equivalent in foreign currency, 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, or its equivalent in foreign currency, 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, or its equivalent in foreign currency, received on any one occasion directly and not through a domestic financial institution, from any person, account or place outside the U.S.

We need to keep records of our business to meet various legal requirements of the Vanuatu and ensure all transactions can be readily reconstructed at any time.

We also need to keep records of our identification and verification procedures and our transactions as well as other AML & CTF activities to comply with the requirements of the AML & CTF Act and Proceeds of Crime CAP 284.

We keep our records in the English language.

## Identification and Verification Procedures

All applications and documents produced to verify identity must be kept for a period of six years after the closure or termination of the account, service or business relationship.

## Transactions

All records generated to complete a transaction should be filed with the application for the transaction and the documents produced to verify identity and the bundle must be kept for a period of six years after the closure or termination of the account, service or business relationship.

For transactions, we generate and keep the following records:

* + - * We give a reference number to the transaction;
			* We record the currency the transaction is in;
			* We record whether the transaction is inbound or outbound;
			* We record the amount;
			* We record the date of the transaction;
			* We obtain and record the name of the Other Party;
			* We keep the application and the identification documents, which also include the address and telephone details of the Customer;
			* We keep any document the Customer has produced for the transaction such as an invoice.

## Case Investigations

All case investigation files must be kept for six years after the date of the investigation.

All suspicious transaction reports to the VFIU must be kept for six years after the date of the report.

## Dealings with the VFIU

Documents generated in the course of dealing with the VFIU must be kept for six years after the date of the report.

Any other reports or documents sent to the VFIU must be kept for six years after the date of the report.

## Governance and assurance documents

Documents generated to manage our AML & CTF obligations, such as this manual, or documents associated with a review of this manual, to the VFIU must be kept for a period of six years after the date of the report.

**Retrieving Records**

All records kept must be able to be easily retrieved and in a form which the VFIU can read them. Electronic records must be capable of being able to be printed out or read on screen.

## 14. Clearing/Introducing Firm Relationships

We will work closely with our clearing firm to detect money laundering. We will exchange information, records, data and exception reports as necessary to comply [with 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, which can be found on [VFIU’s website](https://www.fincen.gov/). As a general matter, we will obtain and use the following exception reports offered by our clearing firm in order to monitor customer activity and we will provide our clearing firm with proper customer identification and due diligence information as required to successfully monitor customer transactions. We have discussed how each firm will apportion customer and transaction functions and how we will share information and set forth our understanding in a written document. We understand that the apportionment of functions will not relieve either of us from our independent obligation to comply with AML laws, except as specifically allowed under the AML&CTF and its implementing regulations.

## 15. 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 STRs); (3) what employees' roles are in the firm's compliance efforts and how to perform them; (4) the firm's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the AML&CTF.

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. We will maintain records to show the persons trained, the dates of training and the subject matter of their training.

We will review our operations to see if certain employees, such as those in compliance, margin and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

## 16. Program to Independently Test AML Program

### a. Staffing

The testing of our AML program will be performed at least annually (on a calendar year basis)] by Han Kang, personnel of our firm, none of whom are the AML Compliance Person nor do they perform the AML functions being tested nor do they report to any such persons. Their qualifications include a working knowledge of applicable requirements under the AML&CTF and its implementing regulations. To ensure that they remain independent, we will separate their functions from other AML activities. Independent testing will be performed more frequently if circumstances warrant.

 **b. Evaluation and Reporting**

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

## 17. 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. Han Kang will review the AML Compliance Person’s accounts.

We only employ people who have the competence to do the job they are employed for.

We look for people with integrity to work in our business.

We monitor our employees for conflicts of interest between their outside life and the work they do in our business.

We have a [code of conduct].

We do not employ people with criminal records.

All our owners have had a police check and we require all our employees to have a police check.

Any transactions that our owners or employees wish to do through our business must be approved by the CO.

We monitor transactions done through our business by persons we know are family or friends of our owners or employees.

We regularly screen our management staff against section 49(1) of the AML&CTF Act.

## Training

All employees must complete the training that we provide annually on this manual and on the requirements of the AML & CTF Act. The training should ensure that employees are aware of the AML & CTF Act, the VFIU Guidelines and the procedures in this manual.

Our training covers:

* + - * The requirements of the AML & CTF ACT;
			* The requirements of this manual;
			* Their responsibilities;
			* How to detect suspicious transactions;
			* The prohibition on tipping off.

## Assurance

The CO will monitor the business for compliance with this manual. This monitoring will include checking that:

* + - * Applicants are being identified properly;
			* Records are being kept;
			* Staffs are attending training and reading compliance newsletters.

The CO will keep records of the checking processes including the dates on which the checking occurred.

## Independent review

The CO will periodically arrange for this manual to be reviewed by an independent person for compliance and adequacy. The CO cannot do this review, nor can a member of her or his staff.

The report of the independent review will be provided to the owner as the CO and the CO will undertake required remediation actions identified in the report if they are practicable and appropriate.

## 18. 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 Christian Kang. Such reports will be confidential, and the employee will suffer no retaliation for making them.

## 19. 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.

## 20. 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 AML&CTF and the implementing regulations under it. This approval is indicated by signatures below.