

CWG MARKETS LTD

VFSC

AML & CTF Procedure Manual

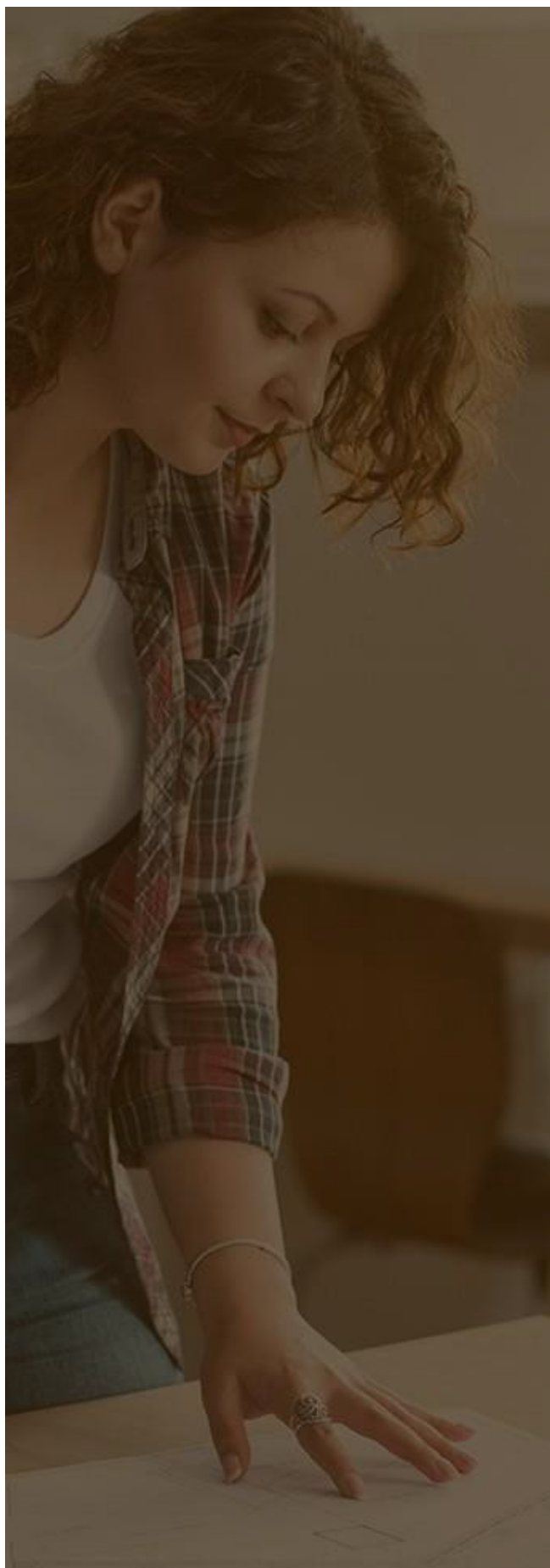


TABLE OF CONTENTS

OVERVIEW	3
MONEY LAUNDERING	3
FINANCING OF TERRORISM	3
OUR POLICY	3
COMPLIANCE OFFICER.....	4
ROLES AND RESPONSIBILITIES	4
TRAINING / AWARENESS	5
CUSTOMER ACCEPTANCE PROCEDURES.....	6
AML & CTF CONTROLS.....	8
RISK Assessment	10
RISK.....	10
DECLINED BUSINESS	13
RECORD KEEPING	13
REPORTING TO THE VFIU	14
OTHER CONTROLS	15
UNFS ACT	16
AUDIT PROGRAM	16
APPENDIX.....	18

OVERVIEW

This Manual provides a blueprint of CWG MARKETS LTD (the company) a financial service company will process for Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF) as an international business once granted to the Vanuatu Financial Services Commission (VFSC) for a principle license to carry on the business of dealing in securities

MONEY LAUNDERING

Definition

Money laundering is a process of concealing the true origin and ownership of illegally obtained money. Principally, it is proceeds of criminal activities such as illicit drugs, corruption, organized crime, fraud, sex trade, forgery, illegal logging/fishing, revenue evasion, counterfeit money, piracy, terrorism etc... which criminals attempt to disguise.

Money laundering process

There is more than one method of laundering money.

Methods can range from purchase and resale of real estate or a luxury item to passing money through a complex web of legitimate businesses and 'shell' companies. In most cases, the proceeds of these criminal activities take the form of cash. There are three stages of money laundering, during which there may be numerous transactions made by launderers that could alert us.

Placement

Placement is the physical disposal of the cash or asset derived from illegal activity. It includes the opening of numerous bank accounts, depositing cash, exporting cash, and using cash to purchase high value goods such as property or businesses.

Layering

Layering is the separation of criminal proceeds from their source by creating complex layering process of financial transactions designed to defeat the audit trail and provide anonymity. It may include telegraphically transferring funds overseas, depositing cash overseas, reselling goods previously with cash.

Integration

Integration provides apparent legitimacy to criminally derived wealth. If the layering process succeeds, integration schemes place the laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate business funds. This may be achieved through a complex web of transfers or income from apparently legitimate businesses previously purchased with the proceeds of illegal activities.

Examples

Examples of the types of transactions that are associated with money laundering and terrorist financing activities are documented in Appendix. These are by no means exhaustive, but are given as an indication of the type of activity involved.

FINANCING OF TERRORISM

Terrorist financing involves collecting and providing funds for terrorist activity. The primary objective of terrorism is 'to intimidate a population, or to compel a Government or an international organization to do or abstain from doing any act'.

The goal of the terrorist or terrorist organization is to maintain financial support in order to achieve their aims, and a successful terrorist group, is one that is able to build and maintain an effective financial infrastructure. Terrorist needs finance for a wide variety of purpose - recruitment, training, travel, materials and setting up safe havens.

Terrorist control funds from a variety of sources around the world and employ sophisticated techniques to move funds between jurisdictions. In order not to be detected, a terrorist group draws in the service of banks and nonbanking institutions and takes advantage of their services products.

2.1 Financing Terrorism and Associated activities

If a known terrorist organization conducts or seeks to conduct a transaction via the business (whether or not the transaction or proposed transaction involves cash), such transaction or proposed transaction is deemed to be a suspicious transaction and the business must submit a report to the VFIU (refer Appendix).

OUR POLICY

Duty of Vigilance

We are expected by the AML & CTF Act and the VFIU to have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the institution from being used, intentionally or unintentionally, by money launderers and terrorism financiers.

The policies and procedures in this manual implement the duty of vigilance expected of us to avoid assisting the process of

laundering and terrorism financing and to react to possible attempts at being used for those purposes.

Principles

- We oppose 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

Our AML & CTF Program is made up of the contents of this manual. Our activities can be described as a series of controls to manage the way we:

- accept applications for transactions;
- monitor the transactions we do for unusual activity that needs further investigation;
- identify events that require us to take further action;
- report certain matters to our VFIU; and
- Keep records of what we do.

Some of the controls we use are embedded in the way our products operate.

Disciplinary action and dismissal

Our staff will face disciplinary action, and possibly dismissal, if they fail to follow the AML & CTF procedures and requirements in this manual. We will dismiss any person who is involved in facilitating money laundering, terrorism financing or who launders money or finances terrorism using our products and services, and we will comply with any law that requires us to report such matters to VFIU and law enforcement. Law enforcement receives our full cooperation in the prosecution of such matters against our staff.

Sometimes customers or transactions involve people we know well, or may involve the owners of this business or someone else close to us. Even if this is the case all our staffs are still expected to follow the procedures in this manual.

Staff should go to the Compliance Officer if they are experiencing difficulties with this area.

COMPLIANCE OFFICER

Compliance officer: Mr. Zhangyu HUA Contact detail: compliance@cwgmarkets.com

Alternate compliance officer: Patrick Joon Leong KOH Contact detail: patrick@cwgmarkets.com

ROLES AND RESPONSIBILITIES

Purpose

It is essential that everyone in our organization understands what they have to do to comply with the requirements of this manual.

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 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 / AWARENESS

New Staff, Employee

The compliance officer will ensure that all new staff members or employees are trained and made aware of this manual before they commenced handling customers and transactions.

Existing Staff, Employees

The compliance officer will ensure all staff members or employees attend AML/CFT training at least annually.

Training Records

Records will be kept of the following for 6 years from the date that training was provided:

- Who was trained;
- What material they were trained with;
- The attendance logs signed by attendees;
- The date they were trained.

CUSTOMER ACCEPTANCE PROCEDURES

Description of our identification and verification process

An individual who wants to establish a business relationship with us is an “Applicant”.

Our application form is designed to capture all the information we need to be able to:

- Establish the identity of the Applicant;
- Assess the risk presented by the application and the Applicant;
- Complete special transactions such as those that involve sending or receiving money from overseas or are above VT1 million or its equivalent in foreign currencies.

Applicants must complete and sign the application form which applies to the transaction they want to do and successfully complete our identification and verification procedure. The purpose of the identification and verification procedure is to reasonably be satisfied that the Applicant is who they claim to be and also to help us understand what risk they represent to us of being involved in money laundering or terrorism financing.

Where an Applicant cannot successfully complete and sign our identification and verification procedure their application must be refused and the matter reported immediately to the CO.

The CO will decide whether the inability to successfully complete our identification and verification procedure should be reported to the VFIU.

The Applicant must not be informed of the reporting of the matter to the CO or what decision is made about reporting the matter to the VFIU. Failure to comply with this procedure may be a criminal offence.

Identification information

All Applicants who are individuals must provide at a minimum the following information on their application form:

- Their true and full name and if they use more than one, all of their names;
- Their date of birth;
- Their occupation;
- Their permanent residential address;
- Their purpose and intended nature of the business relationship with the reporting entity;
- Authorization of any person purporting to act for or on behalf of the customer and the identity of the person

All Applicants must sign their application form with their usual signature and where an automated sales receipt is used, they should 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 to have an understanding on:

- (i) The purpose and intended nature of the business relationship with the reporting entity; and
- (ii) The customer’s beneficial ownership and control structure

Verification information

Veriff - Designated KYC System:

CWG Markets Ltd designates Veriff as its official Know-Your-Customer (KYC) and identity verification system. Veriff performs document and selfie checks, biometric and liveness authentication, sanctions, PEP, and adverse media screening, and provides fraud detection to identify impersonation or identity theft risks.

All verification data and reports generated by Veriff form part of CWG’s Customer Due Diligence record and must be retained for at least six (6) years after account closure. Where third-party introducers are involved, the Compliance Officer must ensure introducers are regulated and AML/CTF compliant, and that Veriff outputs are attached to customer files to demonstrate compliance with Section 18 of the AML/CTF Act. [Financial Intelligence Unit - AML&CTF ACT](#)

Our counter staff are required to verify the identification information using reliable and independent documents. On receiving the application form the counter staff must then ask for the following:

- At least one photographic verification document and at least one non-photographic verification document
- Any two of either Category A documents (see AML & CTF Regulation Order; Schedule 2; Table B).

7.3.2 We accept alternative documents (see VFIU Guideline to Financial Institutions 2008) if the Applicant cannot produce

either the passport or driver's license:

- One category A document and two category B letters; or
- Three category B letters.

If a photographic verification document is unattainable and if so proven then at least 3 non-photographic verification documents is satisfactory.

Applications by visitors to the Vanuatu who cannot produce their passports for identification should be refused because all visitors must at least have a current and valid passport to enter the Vanuatu, and typically would also have a current and valid driver's license.

We do not accept the application of an Applicant that fails to produce photographic identification on more than three occasions unless there are reasonable grounds to believe that they do not possess any document which contains photographic identification. This will only arise in a small number of isolated cases where people are older or live in remote areas of the Vanuatu.

The documents produced by the Applicant for verification of their identity must then be used for the following comparisons:

- Whether the photograph on the document is of the same person as the Applicant;
- Whether the name on the document is the same as provided by the Applicant on the application form;
- Whether the date and place of birth on the document is the same as provided by the Applicant on the application form;
- Whether the address on the document is the same as provided by the Applicant on the application form (addresses on passports are often different because people do move addresses).

Discrepancies

If the photograph, name or date or place of birth on the document is different to the application form then the Applicant should be asked for an explanation. If the explanation is not sufficient then the application should be refused and the matter reported to the CO.

If the name on the document is different to the name on the application because the person has changed their name through deed poll or through marriage then the Applicant must produce their deed poll for change of name or their marriage certificate.

Differences in dates of birth and places of birth should be reported to the CO before accepting the application.

Differences in appearance between the photograph on the document and the Applicant's appearance should be reported to the CO before accepting the application.

Local knowledge

Counter staff who know Applicants personally, or they or someone else in our office 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.

Applicants who are publicly well known because they are prominent public persons are still required to successfully complete the identification and verification procedure, including production of current and valid identification documents.

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

Record making and keeping

The documents produced to verify identification will be photocopied and stored with the application.

Each copy identification document will be stamped or noted with the following words "Original cited [date] by [name]" and the stamp or note initialed by the counter staff person completing the identification and verification procedure. Note - this could be set up on a stamp for staff to use.

The #reverse side of the application form needs to be completed by the counter staff to complete the identification and verification procedure and it includes a statement explaining the reasons where only Category B documents have been accepted for verification.

Persons acting as agents for Applicants who are individuals

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 provide 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 in their own name on behalf of a third party

Each application form asks the Customer to confirm that this transaction is being done by them for their own benefit and using their own money.

If an 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 must successfully complete our identification and verification procedure.

Exception Register

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.

On-going due diligence Process

Ongoing and Event-Driven Customer Due Diligence:

CWG Markets Ltd shall maintain an Ongoing and Event-Driven Customer Due Diligence Program to ensure continuous monitoring of customer activity and compliance with Section 16 of the AML/CTF Act.

Financial Intelligence Unit - AML&CTF ACT

Reverification of customer information shall be conducted immediately upon any prescribed event or material change, including changes in ownership, control, business activity, or identification details, or where suspicious activity is detected. Periodic KYC reviews will occur every 12 months for high-risk customers, every 2 years for medium-risk customers, and every 3 years for low-risk customers.

Transaction monitoring and sanctions-screening alerts shall automatically trigger a compliance review and reverification if warranted. All activities must be reviewed, recorded, and signed off by the Compliance Officer, with records maintained for at least six (6) years and made available to the VFU upon request.

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". 7.10.2 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.

AML & CTF CONTROLS

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.

Enhanced On-Going Due Diligence Process

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

Correspondent Banking Due Diligence:

Before entering any correspondent banking relationship, CWG Markets Ltd shall conduct detailed due diligence consistent with Section 36 of the AML/CTF Act [Financial Intelligence Unit - AML&CTF ACT](#).

The Compliance Officer must complete a structured due-diligence checklist covering ownership, regulatory oversight, AML/CTF controls, and reputation of the correspondent institution. Senior management approval must be obtained and documented prior to engagement.

Written agreements defining each party's AML/CTF responsibilities and reporting obligations shall be retained for at least six (6) years. All correspondent relationships shall be reviewed annually to confirm continued compliance and the absence of shell banks.

When our business engages the services of or has relationships with a cross border correspondent bank we must:

- Adequately identify and verify the person with whom we conduct such a business relationship with
- Gather sufficient information about the nature of the business of the person
- Determine from publicly available information the reputation of the person and the quality of supervision the person is subject to

- Assess the person's anti-money laundering and terrorist financing controls
- Obtain approval from senior management before establishing a new correspondent relationship
- Record the responsibilities of our business and the person whom we will engage business with.

Should the customers of the correspondent bank wish to establish accounts with our business we must ensure that the person:

- Has verified the identity of and is performing on-going due diligence on their customers whom are interested in engaging our services
- Is able to provide to us customer identification data of their customers whom they have referred to our business for use of our services.

RISK Assessment

The Vanuatu Anti-Money Laundering and Counter-Terrorism Financing Act No. 13 of 2014 (the AML/CTF Act) and associated regulations require reporting entities to adopt a risk-based approach to identifying, assessing, and mitigating the risks of money laundering (ML) and terrorist financing (TF). This approach promotes proactive risk management and establishes a strong culture of compliance and ethical conduct throughout CWG Markets Ltd.

In accordance with Section 35 of the AML/CTF Act and VFIU Guidelines, CWG Markets Ltd must conduct and document a comprehensive ML/TF Risk Assessment, taking appropriate steps to identify and assess the risks to which its business is exposed.

CWG Markets Ltd's risk assessment is documented, reviewed annually, and made available to the Vanuatu Financial Intelligence Unit (VFIU) or other competent authorities upon request.

RISK CATEGORIES

- **Customer risk factors** - type, occupation, source of wealth/funds, PEP status.
- **Geographic risk factors** - customer or transaction locations associated with higher ML/TF risk, including sanctioned or high-risk jurisdictions
- **Product and Service risk factors** - complexity, transaction frequency etc.
- **Transaction risk factors** - size, pattern, and purpose of transactions.
- **Delivery Channel risk factors** - non-face-to-face onboarding.

In determining appropriate controls, CWG Markets Ltd considers the size, nature, and complexity of its operations, applying a proportionate risk-based approach consistent with VFIU guidance.

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 this manual.

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 this manual.

Customers with adverse financial report against them

Customers with adverse reports against them are subject to the requirements listed under this manual.

Customers representing or are legal entities/arrangements

Customers representing or are legal entities/arrangement are subject to the requirements listed under this manual.

Product/Service Risk

Large Principal Money Transfers (LPMT) (Money Remitters) >VT 30,000 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 this manual.

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 this Manual

Blacklisted countries:

- Belgium
- Indonesia
- North Korea
- Afghanistan
- Anguilla
- Antigua & Bermuda
- Bahamas
- Belarus
- Belize
- Bolivia
- Bosnia-Herzegovina
- Burundi
- Central African Rep
- Congo, the Democratic Republic
- Cuba
- Ethiopia
- Fiji
- Gaza Strip
- Guinea
- Guinea Bissau
- Haiti
- Iran, Islamic Republic of
- Iraq
- Lebanon
- Libya

- Malaysia
- Mali
- Myanmar
- Nicaragua
- Palau
- Russian Federation
- Somalia
- South Sudan
- Sudan
- Syria
- Ukraine
- United States
- Venezuela
- Yemen

Higher risk countries

The following countries are considered high risk countries:

- Barbados
- British Virgin Island
- Bulgaria
- Burkina Faso
- Cameroon
- Chad
- China
- Hong Kong SAR
- Jamaica
- Kenya
- Kosovo
- Moldova
- Monaco
- Mozambique
- Namibia
- Nigeria
- Panama
- Philippines
- Samoa
- Senegal
- Serbia
- Seychelles
- South Africa
- Tanzania
- Trinidad & Tobago
- Tunisia
- Turkey
- U.A.E
- Uganda
- Vanuatu
- Vietnam
- West Bank (Palestinian Territory, Occupation)
- Zimbabwe

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

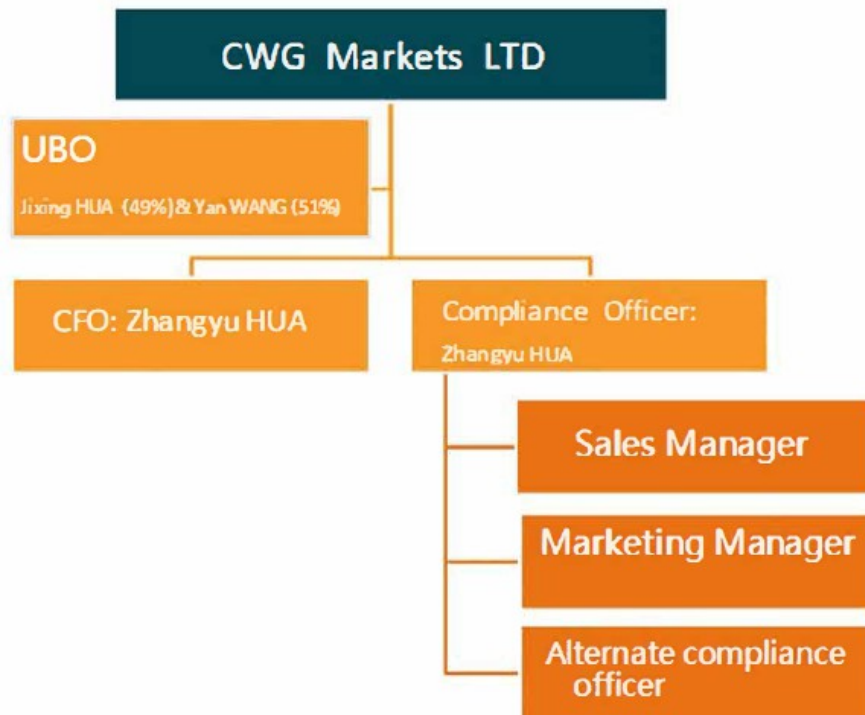
Non-resident applicants are subject to the requirements listed under this manual.

Products/Service Deliver

The Company intends to deal as a principal in (a) shares including: (i) equity interests, (ii) limited partnership interests, and (iii)

units of participation in a unit trust; (b) debt instruments including (i) debentures, (ii) debenture stock, (iii) loan stock, (iv) bonds, (v) certificates of deposit, and (vi) any other instruments creating or acknowledging indebtedness; (c) warrants; (d) options; (e) futures; and (f) CFD. The Company believes that in order to attract a breadth of clients, the full suite of products must be offered and has therefore undertaken to recruit staff with a wealth of experience dealing with such securities.

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 18 years old)
- Customers operating under false or misleading names that we become aware of
- Who does not produce identity or verification within prescribed timeframe

RECORD KEEPING

General

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.

https://customsinlandrevenue.gov.vu/images/legislations/Customs/Others/Proceeds_of_Crime_ActCap_284.pdf

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.

REPORTING TO THE VFIU

Reporting Timelines:

All reports required under the AML/CTF Act must be submitted to the Vanuatu Financial Intelligence Unit (VFIU) within two (2) working days. This includes Cash Transaction Reports (CTR) for any cash transaction exceeding VT 1 million, International Funds Transfer Reports (IFTR) for any cross-border transfer exceeding VT 1 million, and Suspicious Transaction Reports (STR) immediately upon forming a suspicion.

The Compliance Officer shall review and approve all reports prior to submission and record each in the reporting register, including report type, submission date, officer name, and VFIU reference number.

Suspicious Transaction

Transactions or attempted transaction that are suspected to involve proceeds of crime or related to terrorist financing or conducted by prescribed entity or involved terrorist property or are unusual, complex, have no apparent or visible economic or lawful purpose (Appendix - list of possible indicators):

Staff who encounters an unusual transaction or attempted transaction need to report it promptly to the CO and must not proceed further with the transaction unless the CO has given approval.

The staff must not inform the customer that the transaction or attempted transaction is unusual but must refer the Customer to the CO.

Suspicious Activity

Suspicious activity refers to a series of suspicious acts or transactions which are conducted over time and form a pattern or trend.

Staff who encounters a suspicious activity or attempted activity need to report it promptly to the CO and must not proceed further with the activity/transaction unless the CO has given approval.

The staff must not inform the customer that the activity/transaction or attempted activity/transaction is unusual but must refer the Customer to the CO.

Large Cash Transaction

Counter staff must complete the VFIU-issued CTR template (Appendix) for all cash transaction exceeding VT1 million or its equivalent in foreign currency and submit to the CO for her review and sign off.

The CTR must be submitted to the VFIU within: (a) for Vatu currency -2 working days after the transaction or transfer is made; and (b) for foreign currency -2 days after the transaction or transfer is made.

International Currency Transfer

Counter staff must complete the VFIU-issued IFTR Template (Appendix) for all cross border fund transaction exceeding VT1

million or its equivalent in foreign currency and submit to the CO for her review and sign off.

The IFTR must be submitted to the VFIU within: 9a) for Vatu currency -2 working days after the transaction or transfer is made; and (b) for foreign currency-2 days after the transaction or transfer is made.

Reporting process

Our CO is responsible for investigating what has been detected as unusual, deciding if something is suspicious and reporting it to the VFIU. Suspicion is personal, subjective and falls far short of the proof required for a criminal charge in a court. If the CO reports something that turns out not to be suspicious then he or she is protected under the AML & CTF ACT in respect of the report they made. The fact that a report has been made is confidential and no one outside the VFIU and the Vanuatu police and law enforcement will know that a report has been lodged.

Our CO will create a separate file for each investigation other than those which he or she decides on first reading are not suspicious. The CO will keep all the details of the investigation in this file and this file will be stored securely so no other staff can access it.

The CO may consider the following when investigating a transaction or an application:

- Is the size of the transaction consistent with the usual transactions of the Customer;
- Does the transaction make sense in the context of who the Customer is and what they do for a living?
- Has the pattern of transactions done by this Customer changed?
- Where the transaction involves overseas payments, is there a sensible reason why the Customer is engaging in the transaction?

When the CO decides that something is not suspicious, he will record his reasons in the file.

When the CO decides that something is suspicious, he must report the matter in writing to the VFIU within 2 working days after forming the suspicion. The Report must be in the prescribed form in Appendix of this manual.

Our CO must report the large cash transaction and international currency transfer to the VFIU under the prescribed form under Appendix. For transaction in Vatu, the report must be submitted within 2 working days after the transaction is made and for transaction in a foreign currency, the report must be submitted within 2 working days after the transaction is made.

Our CO will keep a register of suspicious transaction reports, recording the date it was lodged and other identifying information. This register will be stored securely so no other staff can access it.

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.

OTHER CONTROLS

Staff Protection and Confidentiality:

CWG Markets VU recognizes the protections granted under Sections 40A, 40B, and 43 of the AML/CTF Act. The identity of staff, officers, or agents involved in preparing or submitting reports to the VFIU is protected and may not be disclosed except to law enforcement or under court order. All staff reporting in good faith are protected from civil or criminal liability.

CWG's reporting obligations take precedence over any contractual or professional duty of confidentiality.

The Compliance Officer shall ensure staff are trained annually on these protections and their legal responsibilities and obligations.

Employee screening and monitoring

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.

UNFS ACT

In order to enable the Company to identify and prevent entering into or continuing in a relationship with a sanctioned target or prospect, the Company screen all customers against relevant sanctions lists, which include the United Nations Financial Sanctions Lists, before entering into a business relationship with them and on a regular and periodic basis following the establishment of the relationship, the Company uses MCO as our planned compliance software.

Actions if there is a match to the sanctions list

We will hold, possess or control property of a designated person or entity, freeze the property immediately and report it to the Sanctions Secretariat within five working days of being notified of the designation; the date of publication of the designation in the Official Gazette; or coming into the possession of the property.

We will also make a report within two working days of a suspicious transaction or activity, or a transaction involving terrorist property, in accordance with the Anti-Money Laundering and Counter Terrorism Financing Act No. 13 of 2014 (AML/CTF Act).

[Financial Intelligence Unit - AML&CTF ACT](#)

We must not:

- Deal with the property, or
- Make property or a financial service available to the designated person or entity, or a person or entity owned, controlled, or acting on their behalf.

False positive

A false positive occurs when an individual or entity with the same or similar name as a designated person or entity is inadvertently identified as being a match to a person or entity on the Consolidated List.

We should:

Conduct an internal investigation to determine whether the match is a false positive. Check birth dates and other identifying information to determine whether the account holder is the designated person or entity.

- If we are unable to determine whether the person is a designated person or entity through an internal investigation, we may seek assistance from the Commissioner of Police to verify whether the person is a designated person or entity.
- If the commission of Police is unable to advise us whether the person is a designated person or entity, you should direct the person to apply directly to the Sanctions Secretariat for assistance using the form available on the VFIU website.

AUDIT PROGRAM

Independent Review and Audit Program:

CWG Markets VU shall maintain an independent AML/CTF review and audit program that assesses the adequacy and effectiveness of its systems, procedures, and controls. Independent reviews/Audit must evaluate compliance with laws, risk management frameworks, and internal staff training.

Mandatory Audits will be conducted on annual basis by a recognized firm of Chartered Accountants.

The Compliance Officer will coordinate all reviews and ensure remediation actions are documented and implemented.

All audit reports and related documents shall be retained for six (6) years and presented to senior management and the Board for oversight.

Objective

The objective of the auditor is to plan the audit so that the audit is conducted effectively.

Responsibility of the Engagement auditor

The engagement partner is responsible for the engagement and its performance. Accordingly, the engagement partner is responsible for planning the audit and may seek assistance from appropriate engagement team members in fulfilling this responsibility. Engagement team members who assist the engagement partner with audit planning also should comply with the relevant requirements in this standard.

Planning an Audit

The auditor should properly plan the audit. This standard describes the auditor's responsibilities for properly planning the audit.

Planning the audit includes establishing the overall audit strategy for the engagement and developing an audit plan, which includes, in particular, planned risk assessment procedures and planned responses to the risks of material misstatement.

Planning is not a discrete phase of an audit but, rather, a continual and iterative process that might begin shortly after (or in connection with) the completion of the previous audit and continues until the completion of the current audit.

Preliminary Engagement Activities

The auditor should perform the following activities at the beginning of the audit:

- Perform procedures regarding the continuance of the client relationship and the specific audit engagement,
- Determine compliance with independence and ethics requirements, and
- Note: The determination of compliance with independence and ethics requirements is not limited to preliminary engagement activities and should be reevaluated with changes in circumstances.
- Establish an understanding of the terms of the audit engagement with the audit committee, Communications with Audit Committees.

Planning Activities

The auditor should evaluate whether the following matters are important to the company's financial statements and internal control over financial reporting and, if so, how they will affect the auditor's procedures:

- Knowledge of the company's internal control over financial reporting obtained during other engagements performed by the auditor;
- Matters affecting the industry in which the company operates, such as financial reporting practices,
- economic conditions, laws and regulations, and technological changes;
- Matters relating to the company's business, including its organization, operating characteristics, and capital structure;
- The extent of recent changes, if any, in the company, its operations, or its internal control over financial reporting;
- The auditor's preliminary judgments about materiality, risk, and, in integrated audits, other factors relating to the determination of material weaknesses;
- Control deficiencies previously communicated to the audit committee or management;
- Legal or regulatory matters of which the company is aware;
- The type and extent of available evidence related to the effectiveness of the company's internal control over financial reporting;
- Preliminary judgments about the effectiveness of internal control over financial reporting;
- Public information about the company relevant to the evaluation of the likelihood of material financial statement misstatements and the effectiveness of the company's internal control over financial reporting;
- Knowledge about risks related to the company evaluated as part of the auditor's client acceptance and retention evaluation; and
- The relative complexity of the company's operations.

Audit Strategy

The auditor should establish an overall audit strategy that sets the scope, timing, and direction of the audit and guides the development of the audit plan.

In establishing the overall audit strategy, the auditor should take into account:

- The reporting objectives of the engagement and the nature of the communications
- The factors that are significant in directing the activities of the engagement team,
- The results of preliminary engagement activities and the auditor's evaluation of the important matters in accordance with

paragraph

- The nature, timing, and extent of resources necessary to perform the engagement.

Client Monies:

- Client's funds are routed through designated 'Client Account' only.
- Proper Segregation of own and client transactions in separate bank account.
- Use of Client account only for purposes allowed by the exchange
- Payments to clients should not be made from own bank account.
- Ensure that clients' funds are not used for own purposes / are not misutilised/are not transferred from one client's account to another client's account.
- Payments to clients are made within the prescribed time limit.
- Payment of dividend amounts to clients and reconciliation of dividend account.
- Running Account of the client is settled as per preference (monthly/quarterly) selected by the client in Running Account authorization letter.
- Periodicity of actual settlement of funds/securities is not more than 3 months/1 month in cases wherein client has consented for quarterly/monthly settlement respectively.
- Member should not deal with clients in cash.
- Internal controls while dealing in dormant client account.
- System for verification of third party cheque.
- In case where aggregate value of banker's cheque / demand draft/ pay order is of Z50,000 or more per client per day, then the same are accompanied with name of bank account holder and number of bank account debited, duly certified by issuing bank as per the provisions of SEBI Circular CIR/MIRSD/03/2011, dated June 9, 2011.
- Member maintains audit trail of the funds received through electronic fund transfers to ensure that the funds are received from their respective clients only.
- Statement of accounts for funds sent to client should contain an extract from the client ledger for funds displaying all receipts/deliveries of funds while settling the account explaining retention of funds.
- If debit balances arise out of client's failure to pay such amount for more than fifth trading day reckoned from date of pay-in, and further exposure is granted to client it would be construed as a funding violation even if fully paid collaterals are available for margins. However, if no further exposure is granted to client from the sixth trading day reckoned from the date of pay-in, such debit balance would not be construed as violation relating to funding.
- Ensure that the funds & securities available in the client bank/s and client beneficiary account/s together with balances available with clearing Member and funds with clearing corporation are not less than the funds and securities payable to the client at all times.
- Verify that Broker is not operating any assured returns schemes and mobilizing deposits from investors.
- Payment for own trades (PRO) are not made from client bank accounts.
- Ensure that Broker has not transferred funds from client bank account to any third party or any other non-client account. Also verify that Broker has not transferred funds to its Group companies/ Associates from client bank accounts.

APPENDIX

Appendix: A SUSPICIOUS TRANSACTION REPORT FORM



VANUATU FINANCIAL INTELLIGENCE UNIT

SUSPICIOUS TRANSACTION REPORT (STR)

PLEASE WRITE IN BLOCK LETTERS

Reporting of suspicious transaction is required under sections 20, 22, 23, 24 and 25 of the AML&CTF Act No. 13 of 2014. Failure to report or reporting false or misleading information may result in fines of up to VT 25 million or 5 years imprisonment or both; or a fine of up to VT 100 million for a corporate body.

PART A — IDENTITY OF CUSTOMERS INVOLVED IN THE SUSPICIOUS TRANSACTION

Person Conducting Transaction

1. Full name (title, given name and surname)			
2. Date of Birth			
3. Occupation, Business or principal activity			
4. Business Address (physical and PO Box)	PO Box:		
	Country:	Phone:	
5. Residential Address (cannot be a PO Box)	Country:	Phone:	
	(Please circle the correct answer)	Yes	No
6. Resident of Vanuatu			
7. Non-Resident- Vanuatu contact address			
8. Is this Person a signatory to an account (s) affected by this transaction	(Please circle the correct answer)	Yes	No

9. Details of Account(s)

a). Account Title / Name:	b). Financial Institution:	Branch:
c). Account Number:	d). Account Type:	

10. How was the Identity of the person confirmed

a) ID Type:	b) ID Number:
c) Issuer:	
11. Is a photocopy of ID documents attached? (Please circle the correct answer)	Yes No

Person On Whose Behalf Transaction Conducted

1. Full name (title, given name and surname)			
2. Date of Birth			
3. Occupation, Business or principal activity			
4. Business Address (physical and PO Box)	PO Box: Country: Phone:		
5. Residential Address (cannot be a PO Box)	Country: Phone: (Please circle the correct answer) Yes No		
6. Resident of Vanuatu			
7. Non-Resident- Vanuatu contact address			
8. Is this Person a signatory to an account (s) affected by this transaction	(Please circle the correct answer) Yes No		
9. Details of Account(s)			
a). Account Title / Name:	b). Financial Institution:		Branch:
c). Account Number:	d). Account Type:		
10. How was the Identity of the person confirmed			
a) ID Type:	b) ID Number:		
c) Issuer:			
11. Is a photocopy of ID documents attached? (Please circle the correct answer) Yes No			

PART B — TRANSACTION DETAILS

12. Transaction Type (eg. Deposit/Withdrawal, Purchase, Sale, Foreign Exchange, Telegraphic Transfer, EFTPOS, etc)	
13. Transaction Date(s)	
14. Transaction Currency	
15. Transaction Amount	
16. Drawer / Ordering Name	
17. Payee / Beneficiary Name	

Give Details of other account(s) affected by this transaction

Account Title / Name		Account Title/Name	
Account Number		Account Number	
Branch		Branch	
Financial institution		Financial Institution	
Name of Signatories		Name Signatories	

NOTE: FOR MULTIPLE TRANSACTIONS OR MULTIPLE FACILITIES PLEASE RECORD DETAILS ON A SEPARATE SHEET

Give details of the nature of and circumstances surrounding the transaction and the reason for suspicion

If insufficient space, attach supplementary sheet. Number of additional pages

Please attached a photo or copy of security tape (if available)

Please attach a photo or copy of recent photo (if available)		
Sex: Male / Female	Race	Clothing
Eye Color	Hair Color	
Build	Age	Distinguishing marks/identifying features (tattoos, facial hair, accent, etc.)
Hair Length/Style	Height (cm)	

(Please tick each boxes below)

- | |
|--|
| |
| |
| |
| |
| |
| |
| |

1. Part A is completed properly
2. Part B is completed properly
3. Part C is completed properly
4. Part D is completed properly
5. Part E is checked

CONFIDENTIAL

Your identity will not be disclosed except for law enforcement purposes or by order of a Court.

Institution Type: (eg. Bank, Solicitor Insurance Company)		Details of Staff Member Conducting Transaction	
		Full Name	

Institution Name

Bank Name:
(if a Bank, include
Bank & Branch No.)

Address

Telephone

Fax

Please forward to: The Financial Intelligence Unit
PMB 9048, Port Vila
Telephone: 23518
Facsimile: 25473
E-mail: frav@vanuatu.gov.vu Or
vfiu@vanuatu.gov.vu

FIU REFERENCE NUMBER

Title/Position

Signature

Date / /

Details of Person Making Report

Full Name

Title/Position

Signature

Date / /

Telephone

Fax

Appendix B: CASH TRANSACTION REPORT FORM**STATE LAW OFFICE****Vanuatu Financial Intelligence Unit****CASH TRANSACTION REPORT
(CTR)**

Reporting of "significant" cash transactions is required by Section 8A of the Financial Transactions Reporting Act [Cap. 268]. Penalties exist for failure to report or to supply full and incorrect information.

**PART A – IDENTITY OF PERSON CONDUCTING
THE TRANSACTION**

1 Full name (title, given names and surname):

Also known as:

2 Date of birth:

3 Country of Birth:

/ /

Day/Month/Year

4 Occupation, business or principal activity:

5 Business address (physical and PO Box):

PMB:

Phone:

Country:

6 Residential address (cannot be a PO Box):

Country:

Phone:

7 NON RESIDENT - Vanuatu contact address:

Country:

Phone:

8 Give details if this person is a signatory to account affected by this transaction

Account Title/Name:

Bank:

Branch:

Account Number:

9 How was the identity of this person confirmed?

ID Type:

ID Number:

Issuer:

10 Is a photocopy of ID document/s attached?

Yes

☐

No

☐

If more than one person involved please provide same details contained in Sections 1 - 11 for each person, where appropriate, and attached

**PART B - DETAILS OF PERSON/ORGANISATION
ON WHOSE BEHALF THE TRANSACTION WAS
CONDUCTED (if applicable)**

12 Full name of person/organisation:

13 Business address (physical and PO Box):

PMB:	Phone:
Country:	

14 Occupation, business or principal activity:

15 Give details if this person is a signatory to account affected by this transaction
Account Title/Name:

Bank:
Branch:
Account Number:

PART C - DETAILS OF THE TRANSACTION
16 Date of transaction:

/ / Day/Month/Year

17 Total amount of this transaction (include cash and any other components of the transaction - If a foreign currency is involved, convert the amount to Vatu).

18 If a foreign currency was involved in this transaction, specify: (eg Australian Dollars, AUD\$ 4000 etc)

Place an 'X' in the appropriate box
☐ **Cash paid IN**
☐ **Cash paid OUT**
PART E - EXPLANATORY NOTES
19 Type of transaction(s) involved

Transfer to another bank	
Travellers Cheques	
Foreign currency	
Bank Cheque	
Account Deposit	
Account Withdrawal	
Bank draft	
Securities	
Precious Stones/ metals/ Pearls	
Other	

- 20 If a cheque/bank draft/money order/telegraphic transfer/transfer of currency or purchase or sale of any security was involved in this transaction, please specify:

Drawer/Ordering Customer:

Payee/Favouree/Beneficiary:

- 21 If another financial institution was involved in this transaction, please specify:

Name of financial institution:

Branch:

Country:

PART D - DETAILS OF THE RECIPIENT PERSON/ORGANISATION (If applicable)

- 22 Full name of person/organisation:

- 23 Business address (physical and PO Box):

PMB:

Phone:

Country:

- 24 Occupation, business or principal activity:

- 25 Reason for transaction (eg payment for imports):

- 26 Details of recipient account (if not already provided):

Account Title/Name:

Bank:

Branch:

Account Number:

- 27 Give details of the nature and circumstances surrounding the transaction if required.

PLEASE PRINT IN BLOCK LETTERS.

- 28 Is additional information attached to this report?

☐

Yes

☐

No

If yes, please Specify:

PART F - REPORTING FINANCIAL INSTITUTION

29 Type of Financial Institution (eg bank):

30 Name of Financial Institution (eg bank):

31 Name of branch or office where transaction was conducted:

32 Business address (physical and PO Box):

PMB:

Phone:

Country:

PART G - FINANCIAL INSTITUTIONS STATEMENT

33 Details of authorised person:
Given Name and Surname:

Job title:

Phone number:

Fax number:

34 This statement is made pursuant to the requirement to report "significant" cash transactions under Vanuatu laws on the grounds detailed in this report.

Signature of authorised person:

(Sign here)

.....
Date:

35 Financial Institutions internal reference number (if applicable).

Send completed forms to:

Vanuatu FIU
PMB 9048
Port Vila
VANUATU

For assistance contact:

Financial Intelligence Unit
Phone: +(678) 23518
Fax: +(678) 25473
Email 1: kbellam@vanuatu.gov.vu

**VANUATU FINANCIAL INTELLIGENCE UNIT USE
ONLY**

Report Number

Authorisation:	
Comments:	

Appendix C: INTERNATIONAL FUNDS TRANSFER REPORT FORM



VANUATU FINANCIAL INTELLIGENCE UNIT

**INTERNATIONAL FUNDS TRANSFER REPORT
(IFTR)**

Reporting of electronic funds transfers into or out of Vanuatu of VUV 1 million or more required by Section 8A of the Financial Transaction Reporting [Cap. 268] Penalties for failure to report or supply full and correct information.

PART A - DETAILS OF THE TRANSACTION	1	Initiating Office	
	2	Date of transmission	
	3	Direction of transmission	
		In	
		Out	
	4	Transaction Ref No:	
	5	Sending Institution:	
		Name of Bank:	
		City	
		Country:	
	6	Receiving Institution:	
		Name of Bank:	
		City:	
		Country:	
PART B - INVOLVED PARTY & INSTITUTION DETAILS	7	Amount Involved. If a foreign Currency was involved in the transaction, specify:	
		Currency:	
		Amount:	
	8	Ordering Customer/organisation	
		Name:	
		Occupation:	
		Address:	
		PO Box:	
		Country:	
		Phone:	
		Account Details:	
		Account Name:	
		Bank:	
		Branch:	
		Account Number:	
		Person who authorised Transfer:	
		Title	
		Name:	
		Position:	
	9	Beneficiary customer/organisation	
		Name:	
		Occupation:	
		Address:	
		PO Box:	
		Country:	
		Phone:	
		Account Details:	
		Account Title:	
		Bank:	
		Branch:	
		Account No:	
		Person identified to receive payment:	
		Title:	
		Name:	

		Position:	
PART C - ADDITIONAL PAYMENT DETAILS	10	Details of payment	
PART D - REPORTING FINANCIAL INSTITUTIONS	11	Any other information	
	12	Type of Financial Institution	
	13	Name of Financial Institution	
	14	Name of branch or office	
	15	Business Address:	
		PO Box:	
		Country:	
PART E - FINANCIAL INSTITUTIONS STATEMENT		Phone:	
	16	Details of authorised person	
		Given names and surname:	
		Job Title:	
		Phone No:	
		Fax Number:	
	17	This statement is made pursuant to the requirement to report international Funds Transfers under Vanuatu laws on the ground as detailed in Part E.	
		Signature of Authorised person:	
	18	Financial Institutions internal reference:	

Send completed forms to:

Vanuatu FIU
PMB 9048
Port Vila
VANUATU

For assistance contact:

Financial Intelligence Unit
Phone: +(678) 23518
Fax: +(678) 25473
Email: kbellam@vanuatu.gov.vu

VANUATU FINANCIAL INTELLIGENCE UNIT USE ONLY

Report Number	
Authorisation:	
Comments:	

Appendix D: Suspicious Activity Report Form



VANUATU FINANCIAL INTELLIGENCE UNIT

SUSPICIOUS ACTIVITY REPORT (SAR)

PLEASE WRITE IN BLOCK LETTERS

Reporting of suspicious activity is required under section 21 of the AML&CTF Act No. of 2014. Failure to report or reporting false or misleading information may result in fines of up to VT 25 million or 5 years imprisonment or both; or a fine of up to VT 100 million for a corporate body.

PART A — IDENTITY OF CUSTOMERS INVOLVED IN THE SUSPICIOUS ACTIVITY

Person(s) Conducting Activity

1. Full name (title, given name and surname)
2. Date of Birth
3. Occupation, Business or principal activity
4. Business Address (physical and PO Box)
5. Residential Address (cannot be a PO Box)
6. Resident of Vanuatu
7. Non-Resident- Vanuatu contact address
8. Is this Person a signatory to an account (s) affected by this transaction

PO Box:		
Country:	Phone:	
Country:	Phone:	
(Please circle the correct answer) Yes No		
(Please circle the correct answer) Yes No		

9. Details of Account(s)

a). Account Title / Name:	b). Financial Institution:	Branch:
c). Account Number:	d). Account Type:	

10. How was the Identity of the person confirmed

a) ID Type:	b) ID Number:
c) Issuer:	

11. Is a photocopy of ID documents attached?
(Please circle the correct answer)

Yes No

Person(s) On Whose Behalf Activity was Conducted

3. Full name (title, given name and surname)

2. Date of Birth

3. Occupation, Business or principal activity

4. Business Address (physical and PO Box)

PO Box:

Country:

Phone:

5. Residential Address (cannot be a PO Box)

Country:

Phone:

(Please circle the correct answer)

Yes

No

6. Resident of Vanuatu

7. Non-Resident- Vanuatu contact address

8. Is this Person a signatory to an account (s) affected by this transaction

(Please circle the correct answer)

Yes

No

9. Details of Account(s)

a). Account Title / Name:

b). Financial Institution:

Branch:

c). Account Number:

d). Account Type:

10. How was the Identity of the person confirmed

a) ID Type:

b) ID Number:

c) Issuer:

11. Is a photocopy of ID documents attached?
(Please circle the correct answer)

Yes No

PART B — DETAIL OF ACTIVITY

12. Activity Type (eg. Deposit/Withdrawal, Purchase, Sale, Foreign Exchange, Telegraphic Transfer, EFTPOS, etc)

13. Activity Date(s)

14. Currency

15. Amount

16. Drawer / Ordering Name

17. Payee / Beneficiary Name

Give Details of other account(s) affected by this activity

Account Title / Name

Account Title/Name

Account Number

Account Number

Branch

Branch

NOTE: FOR MULTIPLE TRANSACTIONS OR MULTIPLE FACILITIES PLEASE RECORD DETAILS ON A SEPARATE SHEET

If insufficient space, attach supplementary sheet. Number of additional pages

Sex: Male / Female		Race		Clothing
Eye Color		Hair Color		
Build		Age		Distinguishing marks/identifying features (tattoos, facial hair, accent, etc.)
Hair Length/Style		Height (cm)		

PART E — CHECKLIST

A. Make sure that you attached the following documentation with your report (If applicable)

(Please tick each boxes below)

1. Copy of an ID (prefer passport, drivers license or Birth certificate or a photo)
2. Copy of the Voucher
3. Copy of the TT/transfer Instruction
4. Copy of dairy note reflecting any
5. copy of the account opening documents
6. copy of the AML questionnaire
7. Provide reference to previous reports made to FIU on the subject

B. Check very carefully that you have completed All sections of this report

1. Part A is completed properly
2. Part B is completed properly
3. Part C is completed properly
4. Part D is completed properly
5. Part E is checked

PART F — FINANCIAL INSTITUTION DETAILS AND PLACE OF TRANSACTION

Institution Type: (eg. Bank, Solicitor Insurance Company)	
Institution Name	
Bank Name: (if a Bank, include Bank & Branch No.)	
Address	
Telephone	
Fax	

Please forward to: **The Financial Intelligence Unit**
PMB 9048, Port Vila
Telephone: 23518
Facsimile: 25473
E-mail: rfay@vanuatu.gov.vu Or
vfiu@vanuatu.gov.vu

FIU REFERENCE NUMBER
PART G — CONFIDENTIAL

Your identity will not be disclosed except for law enforcement purposes or by order of a Court.

Details of Staff Member Conducting Transaction

Full Name

Title/Position

Signature

Details of Person Making Report

Full Name

Title/Position

Signature

Telephone

Fax

Appendix E: Indicators of Suspicious Activity



Money Laundering and Terrorism Financing Indicators

The following is a list of indicators ('red flags') identified from case studies and feedback provided to , which may assist in identifying money laundering and terrorism financing activity. Indicators by themselves may not always be immediately indicative of suspect financial or criminal activity but may give rise to further monitoring and due diligence.

- the transaction was inconsistent with the customer's profile
- associations with multiple accounts under multiple names
- drafts cashed for foreign currency e.g. euros, USD
- cash deposited domestically with the funds subsequently withdrawn from ATMs offshore
- cheques issued to a family member(s) at arms length from person
- cash used to purchase large amounts of gold
- cheques made out regularly to companies and individuals not linked to the account
- deposit of gambling proceeds into a foreign bank account
- depositing multiple large amounts of cash and receiving multiple cheques drawn on that account
- early surrender of insurance policy incurring substantial loss
- elaborate movement of funds through different accounts
- frequent early repayments of loans
- frequent deposits of winning gambling cheques followed by immediate withdrawal of funds in cash
- frequently playing games with low returns but with higher chances of winning
- frequent transfers indicated as loans sent from relatives
- frequent remittance of bearer negotiable instruments e.g. bank drafts, offshore
- funds transferred to a charity fund
- gold transported by the individual but purchased with funds drawn from a company account
- high level of funds placed on stored value cards
- high volume of transactions within a short period
- investment cheques issued to a family member
- insurance policy being closed with request of the payment to be made to a third party accounts
- investment funds sent to 'interesting' countries
- inserting funds into slot machines and immediately claiming those funds as credits
- insurance policy cashed outside the jurisdiction of purchase
- large amount of cash used to purchase insurance policy
- large sums credited into accounts from 'interesting' countries
- large cash deposits used for investment
- large cash deposits into company accounts
- large amounts of currency exchanged for traveller's cheques
- large purchases of gold with transportation of the gold conducted by the individual
- leaving large amounts of cash with a bookmaker and requesting a cheque in return
- large amounts of cash from unexplained sources
- multiple individuals sending funds to one beneficiary
- multiple chip cash-outs on the same day

- multiple cheques cashed into one bank account
- multiple loans obtained over a short period of time with repayments made in cash
- multiple issue of stored value cards and debit cards accessed offshore
- multiple transactions of a similar nature on the same day in different locations
- numerous bank drafts purchased domestically and subsequently deposited internationally
- obtained loan and repaid balance in cash
- purchasing high value assets (e.g. motor vehicles) followed by immediate resale with payment requested via cheque
- purchase of high-value assets e.g. diamond ring, bullion, motor vehicle, property purchase, purchase of an insurance policy followed by immediate surrender
- purchasing and cashing out casino chips with no gaming activity
- physical carriage of cash and/or bearer negotiable instrument out of Australia
- regular sale of large amounts of precious metals and jewellery
- regular sale of large amounts of gold with payment received in cash
- purchase of multiple money orders
- regular use of stored value card to withdraw funds overseas
- regular claims made less than the premium payments
- sale of large amounts of gold from an individual
- structuring cash to purchase traveller's cheques
- structuring the placement of betting transactions
- structuring the purchase of bank drafts
- structuring cash deposits/withdrawals
- structuring chip cash-outs
- structuring the cash used for wire transfers
- transfers from company accounts to private betting accounts
- third party present for all transactions but does not participate in the actual transaction
- transferring funds into third-party accounts
- using third parties to undertake wire transfers
- use of an intermediary to make large cash deposits
- use of intermediary to make insurance policy payments
- unusually large transfer of money from an individual to a business
- use of gatekeepers e.g. accountant and lawyer, to undertake transactions
- use of internet banking to transfer illicit funds into 'mule' accounts
- use of multiple names to conduct similar activity
- use of an offshore company to pay the premiums for an insurance policy taken out privately by individuals
- use of safety deposit box to store large amounts of cash
- use of third parties to undertake structuring of deposits and wire transfers
- unexplained income inconsistent with economic situation
- 'u-turn' transactions occurring with funds being transferred out of a country and then portions of those funds being returned
- use of internet banking to frequently access domestic-based accounts internationally
- use of a remittance dealer to send a large amount of cash
- use of a remittance dealer to send large cash amounts overseas
- use of third parties to purchase gaming chips
- use of gatekeeper (e.g. accountant) to structure deposits and purchase real estate
- use of a third party to gamble proceeds through casinos
- use of companies to move funds under the guise of legitimate transactions
- use of false and stolen identities to open and operate bank accounts
- withdrawal of a large amount of funds in cash
- wire transfers to tax haven countries e.g. British Virgin Islands
- wire transfers from third parties located in tax haven countries