JMI Brokers ltd
(referred as the "Company")

AML & CTF Procedure Manual

25.03.2021

Approved by Savvas Vassiliades acting as director of the Company.

Contents

1. Summary and Definitions

"**Act"** means Anti-Money Laundering and Counter-Terrorism Financing Act No 13 of 2014 as amended from time to time.

"AML & CTF Procedure Manual" means this AML and CTF procedure manual.

"CDD" means customer due diligence.

"**Compliance Officer"** means the compliance officers appointed by the Company.

"**FIU"** means Vanuatu Financial Intelligence Unit.

Duty of vigilance

JMI Brokers LTD is a licensed Financial Services Provider from Vanuatu Financial Services Commission and authorized to carry business on Dealing in Securities under license number 15010

As such, the Company is a reporting entity within the meaning of Article 2 of Anti-Money Laundering and Counter-Terrorism Financing Act No 13 of 2014 as amended from time to time (the **Act**), and the Company has to implement a compliance program in order to identify, prohibit and prevent money laundering and financing of terrorism, and ensure the record keeping and customer identification.

As a consequence, the Company has implemented a compliance program covering the following activities conducted on behalf of any of its customers:

JMI Brokers gives its clients the opportunity to trade a wide range of instruments including Forex Currency pairs, Futures (OTC), Precious Metals, Indices, and Energies that are quoted on major world exchanges.

The implementation of the compliance program of the Company must ensure that the performance of the above activities complies with the Act and its regulations as well as guidance provided by the Vanuatu Financial Intelligence Unit (the **FIU**).

As provided by Article 33 of the Act, the compliance program of the Company has been detailed in this AML and CTF procedure manual (the **AML & CTF Procedure Manual**) which contains internal policies, processes and procedures:

a) to implement the reporting requirements under Part 6 of the Act; and
b) to implement the customer due diligence requirements under Part 4 of the Act; and

c) to implement the record keeping requirements under Part 5 of the Act; and
d) to inform the entity's officers and employees of the laws of Vanuatu about money laundering and financing of terrorism, of the policies, processes and procedures and systems adopted by the entity to deal with money laundering and financing of terrorism; and
e) to train the entity's officers and employees to recognise and deal with money laundering and terrorism financing;
    (a) to vet the officers and employees of the reporting entity to ensure that they are fit and proper persons to engage in anti-money laundering and counter terrorist financing related duties; and
    (b) in the case of a person referred to in paragraph 2(q) (definition of reporting entity) on the role and responsibility of any agent of the person, including the person monitoring the agent's compliance with the person's AML and CTF Procedure Manual; and
f) on the role and responsibility of the AML and CTF Compliance officer; and
g) on the establishment of an independent audit function which is able to test its AML and CTF processes, procedures and systems; and
h) on the adoption of systems by the entity to deal with money laundering and terrorism financing; and
i) on the staff screening, recruitment and retention program.

A well-designed applied and monitored program will provide a solid foundation for compliance with the legislation.

Principles

The AML & CTF Procedure Manual of the Company sets the following principles in order to prevent the Company from assisting the process of money laundering and terrorism financing:

- the Company opposes the crimes of money laundering and terrorism financing and does not tolerate the use of its services for either of these purposes;
- the Company is committed to playing its role in the fight against money laundering and terrorism financing in the Vanuatu and abroad;
- the Company will comply with the laws and regulations of the Vanuatu that relate to AML & CTF;
- the Company will assess and understand the risks arising from doing business;
- the Company will provide its services only for legitimate purposes to persons whose identities have been reasonably ascertain;
- the Company will avoid relationships with those that it reasonably assesses to pose too high a risk of money laundering or terrorism financing;
- the Company will report to the FIU any activity/transaction that it deems suspicious;
- the employees of the Company will undergo AML & CTF trainings in order to

understand their obligations under the Act and the regulations to be able to perform their roles accordingly;

- the Company will monitor and ensure that its customers and their transactions are consistent with the level of money laundering and terrorism financing risk they represent;
- the Company will take into account new and emerging risks that might arise in the future;
- the Company will comply with the requirement under Articles 9, 9A and 9B of the Act to register with the FIU and inform them of any material changes that may occur within its business at any time; and
- the Company will adhere to the requirements under Article 34 of the Act to report to the FIU the appointment of or update on any changes regarding its Compliance Officer (as defined below).

Employees adherence to the AML & CTF Procedure Manual

The Company and all employees will conduct ongoing customer due diligence and account monitoring for all business relationships with customers. It particularly involves regularly reviewing and refreshing Company's view of what its customers are doing, the level of risk they pose, and whether anything is inconsistent with information or beliefs previously held about the customer. It can also include anything that appears to be a material change in the nature or purpose of the customer's business relationship with Company.

Compliance program

The Company's compliance program includes the following components:

- Appointment of a compliance officer;
- Roles and responsibilities within the organization;
- Customer due diligence (identification and verification);
- On-going customer due diligence and transaction monitoring;
- Reporting of financial and suspicious transactions to the FlU;
- Record keeping (customer and transaction);
- Staff information about AML & CTF procedures and staff training/awareness;
- AML & CTF audit function; and
- AML & CTF risk management system.

2. Appointment of a compliance officers

The Company's appointed compliance officer (the **Compliance Officer**)
The Company's appointed alternate compliance officerThe Compliance Officers are senior management members, employed on a full time or part timebasis, with suitable qualifications and experience.

3. Roles and responsibilities within the organization

The Compliance Officer is in charge of:

- Assisting with the development, implementation, and maintenance of an anti-money
- laundering program within our institution JMI Brokers LTD
- Ensuring compliance with current AML regulations,
- Developing and maintaining a risk assessment framework for products and services, clients and customers, and other issues relating to money laundering.
- Keeping and maintaining records of high-risk customers and reporting suspicious
- activities to the authorities.
- Preventing the misuse of the Company by anyone or anybody in illegitimate operations.
- Determining the legal and administrative responsibilities of the Company and of all its
- employees related to anti-money laundering.
- Reporting the suspicious operations which include the probable activities of the
- operations of money laundering and terrorist financing to the competent authorities.
- Training all employees on the rules and internal procedures which have to be observed,
- the risks that they and the Company face and how they can encounter the risks of
- money laundering and terrorist financing through their operations from their positions.
- Accept only those Customers whose identity can be established and verified and whose
- source of funds can be reasonably established to be legitimate.
- Not establish a business relationship, open accounts or maintain accounts for anonymous
- persons or those with fictitious names including anonymous accounts.
- Make every possible effort to know the identity of the customer and the real
- beneficiary (Beneficiary Owner) of the account (i.e. the full name, the place and date of birth and verifying the identity by using valid, official and accredited documents
- "identification data" issued by the official bodies), in addition to the data and
- information available from trusted independent sources.
- Apply a risk-based approach, and enhanced customer due diligence where required.
-

The managers and owners are responsible for:

- Strategic Planning.
- Financial Planning
- Business Management including daily activities monitoring, potential clients if the company, markets, Costs, Revenues, and revenue projections
- Arranging and implementing inspections and audits from third-party organizations and making compliance recommendations based on their findings Overseeing and

implementing an ongoing AML training program for other employees.

The staff is responsible for:

- Marketing and new client's business relation.

4.Customer due diligence requirements

Customer due diligence (identification and verification)

Effective customer due diligence (**CDD**) measures are an essential part of any system designed to prevent money laundering and are a cornerstone requirement of the Act.

A customer will be one of the following:

(a) an **individual**;

(b) a **legal person** – bodies corporate, foundations, partnerships, associations, or any similar bodies that can establish a permanent customer relationship with the Company or otherwise own property.

CDD measures need to be carried out:

- when establishing a business relationship;
- when carrying out an occasional transaction;
- where there is a suspicion of money laundering or terrorist financing;
- where there are doubts concerning the veracity of previous identification information; and when carrying out an occasional transaction that exceeds the prescribed threshold under Article 27 or 28 of the Act (whether done as a single transaction or by way of two or more transactions that appear to be linked).

CDD procedures have to be applied to new customers.

Before entering a business relationship, the Company will make

CUSTOMER DUE DILIGENCE

Effective Customer Due Diligence ("CDD") measures are essential to the management of money laundering and terrorist financing risk. CDD means identifying the customer and verifying their true identity on the basis of documents, data or information both at the moment of starting a business relationship with customer and on an ongoing basis. The customer identification and verification procedures require, first, the collection of data and, second, attempts to verify that data.

During the registration process an individual customer provide the following identification information to the Company:

- Customer's full name.

- Customer's date of birth.
- Country of residence/location of customer.
- Mobile telephone number and e-mail.

After receiving the identification information, the Company's staff should verify this information requesting the appropriate documents.
Appropriate documents for verifying the identity of customer include, but are not limited to, the following:

- For an individual customer: A high resolution scanned copy or photo of pages of a passport or any other national ID, indicating family name and name(s), date and place of birth, passport number, issue and expiry dates, country of issue and Client's signature.;

- For business customers, identity needs to be verified before the relation is entered. In case of a legal entity, each customer needs to provide and disclose:

For a corporate customer: a high-resolution copy of documents showing the existence of the entity, such as Certificate of Incorporation, and, where applicable, Certificate of Change of Name, Certificate of Good Standing, Articles of incorporation, a government issued business license (if applicable), etc.

- A high-resolution copy of a utility bill (fixed-line phone, water, electricity) issued within the last 3 months;
- A copy of a tax or rates bill from a local authority;
- A copy of a bank statement (for a current account, deposit account or credit card account);
- A copy of a bank reference letter.
- When making a funds deposit or funds withdrawal via credit/debit card a customer is required to provide a scanned copy or photo of the credit/debit card (front and back side). The front side of credit/debit card should show the cardholder's full name, the expiry date and the first six and the last four digits of the card number (the rest of the digits may be covered). The copy or scan of the reverse side of credit/debit card should show the cardholder's signature, but the CVC2/CVV2 code must be masked.
- If an existing customer either refuses to provide the information described above or if a customer has intentionally provided misleading information, the Company, after considering the risks involved, will consider closing any of an existing customer's account

The Regulations measures require further research and identification of customers who may pose a potentially high risk of money laundering/terrorism financing. If the Company has assessed that the business relationship with a customer pose a high risk it will apply the following additional measures:

- Obtaining the information relating to the source of the funds or the wealth of the customer will be required (this will be done via e-mail or phone);

- Seek further information from the customer or from Company's own research and third-party sources to clarify or update the customer's information, obtain any
- further or additional information clarify the nature and purpose of the customer's transactions with Company.
- JMI Brokers does NOT accept clients from high risk jurisdictions such as North Korea, Lebanon, Syria,…

- the Company identifies and verifies the customer **against the United Nations Securities Council Resolutions on Terrorism Listing**.

- the Company is using Thomson Reuters Refinit as a tool to identify blacklisted database to proceed with due diligence on any customer

- If an existing customer either refuses to provide the information described above or if a customer has intentionally provided misleading information or if
- The company suspects that the customer is involved in proceeds of crime, a financing of terrorism or a serious offence
- The company suspects that the transaction involves proceeds of crime or may be used for financing terrorism or for committing a serious offence
- The company suspects or have doubts on the veracity and adequacy of the customer identification or information previously supplied then the Company, after considering the risks involved, will consider closing any of an existing customer's account.

On-going customer due diligence and transaction monitoring

CDD must also be applied to existing customers (i.e. those existing prior to the Act coming into force) at appropriate times on a risk-sensitive basis.

The risk assessment for existing business relationships must include a review of the information and documentation held in respect of those customers. Such a review will highlight those relationships where there is doubt about the veracity or adequacy of the information and documentation held.

An appropriate time to conduct CDD procedures on existing relationships will therefore be at any time when the Company becomes aware that any of the circumstances listed below apply either as a result of the risk assessment or otherwise:

- a transaction that is suspected may be related to money laundering or terrorist financing;
- a pattern of behaviour that causes the Company to know or suspect that the behaviour is or may be related to money laundering or terrorist financing;
- transactions or patterns of transactions that are complex or unusually large and which have no apparent economic or visible lawful purpose;
- the Company becomes aware of anything which causes it to doubt the identity of the person who, in relation to the formation of the business relationship, was the applicant for business;
- the Company becomes aware of anything which causes it to doubt the veracity or adequacy of CDD information and documentation already produced;
- a suspicion of money laundering or terrorist financing in respect of a person for whom identification evidence is not already held;
- a change in identification information of a customer;
- a change in underlying principals or third parties on whose behalf a customer acts;
- a change in the beneficial ownership and / or control of a customer;
- an absence of meaningful originator information on wire transfers; or
- in respect of wire transfers, where a one-off payment in excess of VT 1,000,000 is to be made at the request of a non-account holding customer.

The Company has implemented procedures to conduct on-going CDD and on-going monitoring, including:

The Company will conduct ongoing customer due diligence and account monitoring for all business relationships with customers. It particularly involves regularly reviewing and refreshing Company's view of what its customers are doing, the level of risk they pose, and whether anything is inconsistent with information or beliefs previously held about the

customer. It can also include anything that appears to be a material change in the nature or purpose of the customer's business relationship with Company.

5.Reporting of financial and suspicious transactions to the FlU

Suspicious transactions and suspicious activity

Suspicious transactions are financial transactions that the Company has reasonable grounds to suspect are related to the commission of a money laundering offence. This includes transactions that the Company has reasonable grounds to suspect are related to the attempted commission of a money laundering offence.

Suspicious transactions also include financial transactions that the Company has reasonable grounds to suspect are related to the commission of a terrorist activity financing offence. This includes transactions that the Company has reasonable grounds to suspect are related to the attempted commission of a terrorist activity financing offence.

This applies not only when the financial transaction has been completed, but also when it has been attempted.

As a general guide, the Company considers that a transaction may be connected to money laundering or terrorist activity financing when the Company thinks that it raises questions or gives rise to discomfort, apprehension or mistrust.

The context in which the transaction occurs or is attempted is a significant factor in assessing suspicion. This will vary from business to business and from one customer to another. The Company valuates transactions in terms of what seems appropriate and is within normal practices in its particular line of business, and based on its knowledge of its customer. The fact that transactions do not appear to be in keeping with normal industry practices may be a relevant factor for determining whether there are reasonable grounds to suspect that the transactions are related to money laundering or terrorist activity financing.

Money laundering offence

Under Vanuatu law, a money laundering offence involves various acts committed with the intention to conceal or convert property or the proceeds of property (such as money) knowing or believing that these were derived from the commission of a designated offence. In this context, a designated offence means most serious offences under the Penal Code or any other Vanuatu act. It includes, but is not limited to those relating to illegal drug trafficking, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation, tax evasion and copyright infringement.

A money laundering offence may also extend to property or proceeds derived from illegal activities that took place outside Vanuatu

Terrorist activity financing offence

Under Vanuatu law, terrorist activity financing offences make it a crime to knowingly collect or provide property, such as funds, either directly or indirectly, to carry out terrorist crimes.

This includes inviting someone else to provide property for this purpose. It also includes the use or possession of property to facilitate or carry out terrorist activities.

Reporting process

In case of suspicious transaction or activity:

Effective Customer Due Diligence ("CDD") measures are essential to the management of money laundering and terrorist financing risk. CDD means identifying the customer and verifying their true identity on the basis of documents, data or information both at the moment of starting a business relationship with customer and on an ongoing basis.

In case of suspicious transaction or activity then customers provide the following identification information to the Company:

- 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
- Supporting documents such as invoices, purchase orders, contracts.

After receiving the identification information, the Company's Alternate Compliance officer Mr. Shokri Ibrahim should verify this information requesting the appropriate documents and report that to the compliance officer Mr. Ismail Ismail.

Both Alternate Compliance officer and the compliance officer Mr. Ismail Ismail. Decide after whether to approve or not that transaction.

All reports are kept to be easily retrieved and in a form which the VFIU can read them such as soft copies and electronic records which can be printed out or read ton screen.

In case of Large Cash Transaction

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

Confidentiality

the Company does not inform anyone, including the customer, about the contents of a suspicious transaction report or even that the Company has made such a report.
the Company will not be requesting information from the individual conducting or attempting the transaction that the Company would not normally request during a transaction.

As provided by Article 32A of the Act, the Company must not disclose any information to any other person:

(a) that a reporting entity, or the supervisory body or auditor of a reporting entity, has formed a suspicion in relation to a transaction or an attempted transaction, or an activity or attempted activity; or
(b) that a report under this Act is made to the FIU; or
(c) that information under this Act is given to the FIU; or
(d) if the person to whom the information is disclosed may reasonably be expected to infer any of the circumstances in paragraph (1) (a), (b) or (c).

The above does not apply if the disclosure is made to an authorized person identified under Article 32A (1) and (2).

As provided by Article 32B of the Act, the Company commits an offence punishable upon conviction if by making a report or providing information required under Part 3, 4, 5, 6, 7 or 8 of the Act:

(a) we make any statement that we know is false or misleading in a material particular; or
(b) we omit from any statement any matter without which we know that the statement is false or misleading in a material particular.

6.Record keeping (customer and transaction)

Record keeping is an essential component of the audit trail procedures to ensure that tracing and confiscation of criminal and terrorist funds can be made.

The records that the Company prepares and keeps are such that :

- supervisors, auditors and law enforcement agencies will be able to assess the effectiveness of the AML & CTF policies and procedures that are maintained by us (including but not limited to the AML & CTF Procedure Manual, AML & CTF assessment and AML & CTF audit reports);
- any transactions or instructions effected via the Company on behalf of any individual customer can be reconstructed;
- any customer can be properly identified and located during the customer due diligence process, enhanced customer due diligence and on-going monitoring process;
- a CDD profile can be established for all customers for whom there is a business relationship (including but not limited to records referred to under Articles 15(2), 17(2) and 18(2));
- all suspicions received internally, and suspicion reports made externally, can be identified (including but not limited to any reports under part 6 of the Act and any enquiry relating to money laundering and the financing of terrorism made to the FIU);
- the rationale for not passing on any internal suspicions to the FIU can be understood; and
- the Company can satisfy, within a reasonable time frame, any enquiries or court orders from the appropriate authorities as to disclosure of information.

The Company shall keep records Soft Copies/Hard Copies and electronic records at two different Cloud storage, Data Centres and dedicated servers which allow us to retrieve quickly the records once needed. for a period of six (6) years after the completion of transaction, the date of the report, the date of investigation, or the termination of business relationship (as applicable).

7. Staff information about AML & CTF procedures and staff screening / training / awareness

The Company establishes, maintains and operates appropriate procedures in order to be satisfied of the integrity of any new directors or partners or managers and all new employees.

As a result, the Company has the following recruitment process:

- We only employ qualified People to do the job they are employed for.
- We look for people with integrity to work in our business.
- 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.
- We conduct Three interviews before final approval on any candidate.
- We take the three interviews by phone, Video Call and finally personal meeting.

In order to discipline the employees:

- To provide Non-Criminal Record on Annual basis.

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.

In order to vet the existing employees:

All Company employees, managers and directors must be aware of this policy. Employees, managers, and directors who are engaged in AML related duties must be suitably vetted. This includes a criminal check done at the time of employment and monitoring during employment. Any violation of this policy or an AML program must be reported in confidence to the AML Compliance Officer, unless the violation implicates the AML Compliance Officer, in which case the employee must report the violation to the Chief Executive Officer.

Employees who work in areas that are susceptible to money laundering or financing terrorism schemes must be trained in how to comply with this policy or the AML program. This includes knowing how to be alert to money laundering and terrorism financing risks and what to do once the risks are identified.

The effectiveness of the compliance program of the Company depends on how well the employees understand their responsibilities. This is the reason why the Company has implemented steps to ensure that all employees are aware and trained.

The Company provides AML training to employees who will be dealing with customers or will be involved in any AML checking, verification, or monitoring processes. The Company may conduct its training internally or hire external third-party consultants.

Each person employed within the Company is assigned a supervisor who teaches him or her in relation to all policies, procedures, customer documentation forms and requirements, forex markets, trading platforms, etc. There is a training plan for each new employee and tests which are being held for 2-3 months (depending on level within the business).
The Company's AML training programs is aimed to ensure its employees to receive appropriate training level with regards to any possible AML/TF risks.

Content of training

1. The Company's AML and risk awareness training includes the following content:
2. The Company's commitment to the prevention, detection and reporting of ML and TF crimes.
3. Examples of ML and TF that have been detected in similar organizations, to create an awareness of the potential ML and TF risks which may be faced by the Company's employees
4. Well known or recognized typologies, especially where made available by the FATF or AML Supervisors.
5. The consequences of ML and TF for the Company, including potential legal liability.
6. The responsibilities of the Company under the AML Act and Regulations.
7. Those responsibilities of employees as identified in this AML Policy, and how employees are expected to follow the Company's AML procedures.

8. How to identify and report unusual activity that may be a suspicious transaction or attempted transaction.
9. The rules that apply against unlawful disclosure of suspicious transactions ("tipping off").

8.AML & CTF audit function

The procedure for conducting an independent AML & CTF audit is to have approval from senior management for the audit to be conducted

Here is what we expect from an AML audit.

- A review of the written **AML** compliance policies.
- Testing of the **AML** compliance procedures.
- Customer Identification Program (CIP) review.
- Review of customer transactions and client files.
- OFAC checks.
- Evaluation of employee training.
- Review of automated monitoring systems.
- the audit is conducted annually
- the audit report will be saved or filed on hard copies/Soft Copies

9.AML & CTF risk management system

Determining the risk

The Company undertakes an assessment to estimate how vulnerable it is to money laundering and terrorist financing. In doing so the Company considers the extent of its exposure to risk by reference to the nature, scale and complexity of its activities, its customers, products and services and the manner in which the Company provides these products and services to its customers, and the reliance which is placed on any third parties for elements of the CDD collected.

1. The Company does NOT have nor offer any business relation with customers of **Higher risk countries.**
2. The Company does NOT offer its services to clients from Unites States, Canada, nor Vanuatu

3. When making a funds deposit or funds withdrawal via credit/debit card a customer is required to provide a scanned copy or photo of the credit/debit card (front and back side). The front side of credit/debit card should show the cardholder's full name, the expiry date and the first six and the last four digits of the card number (the rest of the digits may be covered). The copy or scan of the reverse side of credit/debit card should show the cardholder's signature, but the CVC2/CVV2 code

must be masked.

If an existing customer either refuses to provide the information described above orif a customer has intentionally provided misleading information, the Company, after considering the risks involved, will consider closing any of an existing customer's account.

- The Company shall keep records Soft Copies/Hard Copies and electronic records.

Organizational Risk

• The nature and fundamentals of the transaction and the market underlying such transactions
• The extent of the economic risk to which you are exposed as a result of such transactions.

Customer Risk

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

According to the practices of the Company, some sub-categories of customers may be categorized as follows:

- Politically exposed person will be identified, rated asa high risk and classified as "higher risk Jurisdictions".
- The Company shall not conduct business with higher risk Jurisdictions.

Adequate on-going CDD on existing customers and enhanced CDD on new customers should be put in place when there are identified with high risks.

Business risk

• The nature and fundamentals of the transaction and the market underlying such transactions
• The extent of the economic risk to which you are exposed as a result of such transactions

Product/service risk

Highly Volatile Instruments

Many instruments are traded within wide ranges of intraday price movements so the Client carefully consider the fact that there is not only high probability of profit, but also of loss.

Activity risk

MARKET DATA AND INFORMATION

inaccuracy, error or delay in, or omission of any such data, information or message or the transmission or delivery of any such data, information or message.

Delivery Channels

"Online Service" includes all software and communication links.
Any loss or damage arising from or occasioned by any such inaccuracy, error, delay, omission, non-performance, interruption in any such data, information or message, due to either to any negligent act or omission or to any condition of force majeure or any other cause , whether or not within our or any provider's control.

Jurisdictions

- The Company does NOT have business relation with customers of **Higher risk countries.**
- The Company does NOT offer its services to clients from Unites States Offer, Canada, nor Vanuatu

Enhanced CDD and on-going transaction monitoring must be done on customers and transactions originating from non-higher risk jurisdictions.

10. Procedure Manual

- formulating and documenting the Procedure Manual
- reviewing and approving the Procedure Manual
- familiarizing staff on the purpose and contents of the Procedure Manual
- recording and filing the Procedure Manual]

UNFS Act

JMI Brokers LTD does not contravene any prohibition under Part 3 of the UNFS Act No.6 of 2017, as the company correctly screens its list of customers against the United Nations Financial sanctionsList through Thomson Reuters compliance software, which is being implemented currently, including the UNFS list. Our compliance program is adequatly chosen based on who our customers are and the kind of business we operate.

In case our company holds, controls, possesses property of a designated person/entity, we report itto the Sanctions Secretariat within five working days of being notified of the designation.

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

Failure to make a report is an offence under both the UNFSA and the AML/CTF Act.

Our company must not deal with the property, or make property or a financial service available tothe designated person or entity, or a person or entity owned, controlled or acting on their behalf.

In some cases, someone might claim there has been a false positive match to the Consolidated List. 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 ConsolidatedList.

If our company gets approached by an individual or entity that believe they have had their assetsfrozen in error, we conduct an internal investigation in order to determine whether the match is afalse positive by checking birth dates and other identifying information.

If we were 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 toverify whether the person is a designated person or entity.

If the Commissioner of Police is unable to advise us whether the person is a designatedperson or entity, we direct the person to apply directly to the Sanctions Secretariat for assistance using the form available on the VFIU website.