ANTI-MONEY LAUNDERING,

COUNTER-FINANCING OF TERRORISM

AND

KNOW YOUR CLIENT

POLICY MANUAL

January 2020

Approved by JMMB Group Board of Directors

January 30, 2020

JMMB

ANTI-MONEY LAUNDERING AND KNOW YOUR CLIENT POLICY MANUAL

TABLE OF CONTENTS

1 POLICY STATEMENT

ANTI-MONEY LAUNDERING & COUNTER FINANCING OF TERRORISM POLICY STATEMENT

JMMB will not allow its products, services or facilities to be used as a vehicle for criminal activities. JMMB is committed to conducting business in conformity with high ethical and professional standards and will adhere to all laws and regulations which govern its operations. We are therefore determined to maintain the reputation of JMMB and to prevent it from becoming a vehicle for, or victim of, any illegal activity.

The Board and Management of JMMB are committed to the establishment and implementation of programmes, policies, procedures and controls to detect and prevent money laundering and terrorist financing activities.

We are focused on developing a culture in which the highest priority is given to ensuring compliance with the Proceeds of Crime Act and the Guidance Notes of both the Bank of Jamaica and the Financial Services Commission.

JMMB is committed to the following actions:

(1) JMMB will ensure that adequate policies and procedures are implemented to document and verify the true identity of all clients in accordance with its policies and all applicable regulations.
(2) JMMB will ensure that adequate policies and procedures are in place to identify, prevent and detect suspicious transactions or activities through the adoption of adequate due diligence policies with emphasis on knowing clients and their businesses.

(3) Through ongoing training and education, JMMB will ensure that all employees understand and are aware of:

- the current as well as new and developing AML and CFT laws and regulations, standards and guidelines both locally and internationally
- their legal obligations and responsibilities to prevent and detect money laundering and the financing of terrorism
- new money laundering and terrorist financing techniques, methods, typologies and trends.

(4) JMMB will implement adequate policies, procedures and controls to ensure that its products, services and facilities are not used as vehicles for illegal activities.

(5) JMMB will implement adequate policies and procedures to ensure compliance with all governing regulations, guidelines and best practices relating to Anti-Money Laundering and Countering the Financing of Terrorism.

(6) JMMB will co-operate with the CTD , the regulators and any other law enforcement agencies to which it is has an obligation, in the prevention and detection of money laundering and the financing of terrorism.

(7) JMMB will implement procedures to ensure that adequate records are maintained to support all transactions and client KYC verification in accordance with the regulations and JMMB's policies.

(8) JMMB has appointed a Group Compliance Manager who is responsible for ensuring the establishment and maintenance of an effective Anti-Money Laundering and Counter Financing of Terrorism Program meme.

It is important that all employees of JMMB are aware of and fully understand those actions that may be violations of regulations and guidelines relating to Anti-Money Laundering and

Countering Financing of Terrorism, and to report any potential violation in the manner set forth in this policy.

As a result, team members must note and report the following to the Compliance Analysts or Group Compliance Manager:

- Any unusual transaction that is disproportionate to the client's known business activity.
- Insufficient information given by the client who wants to open an account or conduct business.

Violations of the Proceeds of Crime Act, the Money Laundering Regulations and Guidelines from BOJ and the FSC include:

- Structuring transactions to avoid AML/CFT reporting requirements.
- Failing to prepare or file the required Suspicious Transaction Reports or preparing inaccurate reports
- Aiding money laundering activities
- Advising clients involved in any of these activities.

JMMB will not tolerate any violation of the laws or the regulations in the conduct of its business or related activities.

Any employee who exposes any company within the JMMB Group to undue risk through violation of any policy or procedure is subject to disciplinary action which may include termination.

If an employee intentionally violates any applicable AML/CFT Law or Regulation, this will be reported to regulatory and law enforcement officials in accordance with the Proceeds of Crime Act, the Money Laundering Regulations and the Guidelines issued by the Bank of Jamaica and the Financial Services Commission.

2 INTRODUCTION - APPLICABILITY OF POLICY

The Proceeds of Crime Act, 2007 (hereinafter referred to as the Act) and the Proceeds of Crime (Money Laundering Prevention) Regulations, 2007 (hereinafter referred to as the Regulations) require financial institutions to implement money laundering prevention and detection policies and procedures. In addition JMMB has found the need to ensure that our policies and procedures are compliant with the Foreign Account Tax Compliance Act (FATCA) and any other relevant Acts and regulations.

In light of this obligation, the Board of Directors of JMMB Group Limited has ratified the following policy and directs that it be complied with by all team members of branches, departments and Jamaican subsidiaries of JMMB Group Limited (hereinafter collectively referred to as "JMMB").

Overseas subsidiaries will be governed by the Anti-Money Laundering (AML) and Know Your Client (KYC) laws, regulations and guidelines dictated by the respective resident countries. Where there are no legal or regulatory guidelines of the resident countries for specific areas considered critical to the AML & KYC programme, this policy document should be adopted for those specified areas of operations.

Where their regulators so require, a banking subsidiary or a subsidiary in another jurisdiction may adopt their own AML / KYC policy.

This policy should be read in conjunction with the applicable AML/KYC policies and procedures, including the risk assessment manual, specific to the JMMB subsidiaries.

2.1 POLICY OBJECTIVES

The Board of Directors and Management of JMMB are committed to ensuring the highest ethical and professional standards while conducting our business activities.

JMMB is therefore committed to knowing its clients as well as their banking, investment, remittance, insurance and fund management activities by adopting sound business practices that will detect and identify unusual activities in a timely manner.

The goal is to protect JMMB's reputation and therefore protect it from being used as a vehicle for or from being a victim of any illegal activities committed by its clients.

In order to achieve this goal, we are focused on developing a culture in which the highest priority is given to achieving compliance with the relevant regulations and guidelines.

The primary objectives are as follows:

1) To ensure compliance with the Proceeds of Crime Act, The Proceeds of Crime (Amendment) Act 2013, The Proceeds of Crime (Money Laundering Prevention) Regulations 2007, the Terrorism Prevention Act and other laws impacting on JMMB's Compliance programme and the guidelines issued by the regulators.

2) To protect the reputation and integrity of JMMB by implementing adequate controls and systems to prevent the possibility of the products and services of JMMB being used as vehicles for illegal activities.

3) To ensure that all team members are aware of and understand the issues in relation to money laundering and the financing of terrorism and their responsibilities and obligations under the policies of JMMB and the regulations.

4) To ensure that all team members will be able to recognize unusual and/or suspicious transactions, understand how to report such transactions and are aware of the penalties and sanctions for non-compliance.

5) To ensure that its subsidiaries situated outside of Jamaica are aware of the provisions of the Jamaican AML/CFT laws and the provisions of the guidance notes from regulators on AML/CFT, insofar as the dealings of such subsidiaries with the local registered companies will be affected by the laws and guidance notes.

2.2 POLICY OVERVIEW

JMMB operates within the global financial services industry which is highly regulated and is a key stakeholder in the fight against money laundering and terrorist financing activities.
JMMB is committed to preserving its reputation in the global financial community through the implementation of programmes, policies and systems to strengthen its anti-money laundering and counter financing of terrorism frameworks. As a regulated group of companies, JMMB acknowledges the importance of its role in ensuring the safety and soundness of its operations and furthering efforts to combat money laundering and terrorist financing.

Jamaica's Anti-Money Laundering Regulatory Framework continues to be strengthened with the introduction of new laws, expansion of the role and powers of enforcement agencies and revision of existing laws and regulatory guidelines. Failure to comply with these regulations and guidelines may result in significant penalties or prosecution under the Proceeds of Crime Act and the Terrorism Prevention Act, as well as regulatory action by the Bank of Jamaica and the Financial Services Commission.

In an effort to protect JMMB against the possibility of being used for illegal activities, JMMB has established and implemented these policies and procedures, which are applicable to all subsidiaries, to prevent and detect Money Laundering and Terrorist Financing.

This policy may change from time to time in response to new or revised regulations, in order to ensure the effectiveness and efficiency of the JMMB operations. This policy is subject to annual review by the Board of Directors of the companies within the JMMB Group of Companies.

The implementation of the Anti-Money Laundering, Counter-Financing of Terrorism and Know Your Client Policies and Procedures are to ensure that reasonable assurance is given that the risk to JMMB from money laundering and terrorist financing is minimized. The policy, and where necessary the associated procedures, will be submitted to the Competent Authority for review before it is signed off by the Board.

The Anti-Money Laundering, Counter-Financing of Terrorism, Know Your Client Policy and Client and Account Management Guidelines will apply to all operations within the JMMB Group in conjunction with any specific AML legislation within the different jurisdictions.

The JMMB Anti-Money Laundering, Counter-Financing of Terrorism, Know Your Client Policy is organized into three sections as follows:

Section I: Anti-Money Laundering and the Counter-Financing of Terrorism
Section II: Know Your Client
Section III: Client Acceptance and Relationship Management

2.3 LIST OF ABBREVIATIONS USED THROUGHOUT THE DOCUMENT

TERM	DEFINITION
AML	Anti-Money Laundering
ARA	Asset Recovery Agency
BOJ	Bank Of Jamaica
CCO	Chief Compliance Officer
CDD	Client Due Diligence
CFATF	Caribbean Financial Action Task Force
CFT	Counter-Financing Of Terrorism
CTD	Chief Technical Director
DPP	Director Of Public Prosecutions
EDD	Enhanced Due Diligence
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FID	Financial Investigations Division
FSC	Financial Services Commission
INDIV	Individuals
KYC	Know Your Client
KYE	Know Your Employee
MLP	Money Laundering Prevention
ML/TF	Money Laundering / Terrorist Financing
OFAC	Office Of Foreign Assets Control
PEP	Politically Exposed Persons
POCA	Proceeds Of Crime Act
RM	Relationship Managers
SAR	Suspicious Activity Report

TERM	**DEFINITION**
STR	Suspicious Transaction Report
TIN	Taxpayer Identification Number
TPA	Terrorist Prevention Act
TRN	Tax Registration Number
TTR	Threshold Transaction Report
UTR	Unusual Transaction Report

2.4 JMMB AML COMPLIANCE POLICY

JMMB is required to implement an effective AML Compliance Policy to ensure compliance with all laws, regulations, and guidelines in relation to AML and the CFT. JMMB's AML Compliance Policy outlines the following areas which are detailed further in this and other relevant sections of the policy:

- The documentation, verification and due diligence requirements for new and existing clients (see sections on Know Your Client Policy).
- The nature and frequency of account and transaction monitoring transactions.
- The frequency, nature and scope of AML compliance testing.
- The nature and scope of AML training.
- Compliance risk assessments for new products and services.

2.5 JMMB KNOW YOUR CLIENT POLICY

JMMB is required to establish a KYC Policy which is a critical component in the achievement of AML compliance. JMMB's KYC Policy focuses primarily on client identification requirements, client due diligence, Know Your Employee (KYE) principles, the monitoring of accounts and identification of unusual and/or suspicious activity. (See *detailed requirements in Section II: KYC Policy*)

The Proceeds of Crime (Money Laundering Prevention) Regulations allows for sharing of information across the member companies within a group of companies as well as group policies, procedures and controls to facilitate the prevention and detection of money laundering. This excludes information that is otherwise protected from disclosure under the Act or any other law. Companies within the JMMB Group may therefore operate with one group AML/KYC policy with a view to preventing and detecting money laundering. Information sharing within the group is therefore permitted, save and except for protected information.

Under the law a "responsible entity" has the responsibility for the development and implementation of anti-money laundering, or terrorist financing prevention, policies and procedures for the group of companies. JMMB Group Limited is the responsible entity.

3 ROLES AND RESPONSIBILITIES

The following outlines the roles and responsibilities of the Board of Directors, Committees of the Board, Senior Management, The Risk, Culture and Human Development Team, the Compliance Department, Team members who are critical to the AML and CFT programme. The specific responsibilities for each grouping are as follows:

3.1 THE BOARD OF DIRECTORS

The ultimate responsibility for compliance with the AML/CFT Policy and Procedures lies with the Board of Directors.
In order to fulfil its obligations, the responsibilities of the Board of Directors include:

- mandating a risk assessment of all its business relationships and one-off transactions with a view to determining the business relationships or one-off transactions which are high risk;
- ensuring that policies, controls and procedures are in place that enable the organization to manage and mitigate effectively the risks that have been identified (either by the country or by the financial institution);
- monitoring the implementation of those controls to ensure that they are consistent with Jamaican laws and guidance from the Competent Authorities;

- ensuring that the Human Resources Manual adequately captures disciplinary action for non-compliance with regulatory requirements;
- approving AML/CFT policies and program memes and any amendments thereto;
- appointing a "Nominated Officer" / "Compliance Officer";
- ensuring the establishment of a compliance plan;
- requiring and reviewing compliance and audit reports indicating regulatory compliance, as well as, compliance with internal controls with corrective measures instituted (where necessary).
- ensuring that training is executed for all team members and members of the various Boards of Directors

3.2 THE AUDIT COMMITTEE

The Board has delegated responsibility for overseeing the AML compliance function to the Audit Committee. The role of the Audit Committee in relation to JMMB's AML/CFT Policy includes:

- Reviewing and recommending proposed amendments to JMMB's AML/CFT Policy Manual before they are submitted to the Board of Directors for approval.
- Reviewing internal and external audit reports of the AML/CFT Program meme.
- Reviewing reports prepared by the Country Compliance Officer or designate in the organization's compliance programme and making appropriate recommendations to the Board of Directors in respect thereof.
- Reviewing the results of AML examinations, compliance reviews, audits and independent testing, as well as corrective actions planned or taken in response thereto.
- Monitoring on-going AML activities and issues by receiving and reviewing reports provided by the Compliance Department on a regular basis.

3.3 SENIOR MANAGEMENT – WITH REGULATORY ACCOUNTABILITY

For the purposes of this Policy, "Senior Management" is comprised of JMMB's Executive Team Leaders and Senior Team Leaders or any other role analogous with these positions. In collaboration with Compliance they are responsible for:

- conducting a risk assessment of all business relationships and one-off transactions with a view to determining the business relationships or one-off transactions which are high risk;
- establishing policies and procedures for preventing and detecting money laundering and the financing of terrorism and which mitigate effectively the risks that have been identified (either by the country or by the financial institution);
- establishing the compliance plan providing for ongoing independent review and testing of team member compliance (approved by the Board);
- establishing resources adequate for the day-to-day monitoring of compliance;
- prohibiting the entities within the Group from facilitating the retention or usage of tainted funds;
- being aware of exceptions and following up to ensure corrective action is immediately instituted;
- submitting compliance reports at meetings of the Board of Directors
- providing approval before the company enters into or continues a relationship with a high-risk person

SENIOR MANAGEMENT - OTHER

Senior Management must ensure that controls are in place to ensure that detection and reporting procedures are being followed and these should include:

- Clear lines of authority and responsibility;

- Segregation of duties;
- Job rotation;
- Establishment of limits;
- Monitoring of activities;
- Identification and monitoring of key risks;
- Ensure that the new product approval process is adhered to

3.4 CULTURE AND HUMAN DEVELOPMENT TEAM

The responsibilities of the Culture and Human Development Team (CHDT) relating to the AML programme include:

- Applying appropriate disciplinary action, including termination of employment when team members fail to comply with AML laws or regulations or AML policies and procedures.
- Working with the business units to determine how best to incorporate compliance in performance evaluations and incentives.
- Implementing a comprehensive screening process, involving investigation of background, honesty and competence of team members prior to employment and during employment as may be required.
- Executing the KYE process to ensure that all team members maintain fit and proper status.
- Working with the Compliance Department in ensuring that all team members receive the annual AML Training.
- Ensuring that there are systems in place for evaluating employment and the financial history of team members.
- Advising the regulators in writing immediately upon the termination of the employment of any dealer representative, investment advisor or bank representative.

3.5 THE COMPLIANCE DEPARTMENT

Through the leadership of the Group Chief Compliance Officer, the department provides company-wide AML/CFT oversight and support to JMMB's business and support units in establishing and implementing procedures for compliance with the applicable AML laws and regulations and regulatory guidelines. The primary responsibilities of the Compliance Department include:

- Evaluating laws, guidance notes and regulations, with the guidance of external counsel, to determine their applicability to JMMB.
- Performing company-wide risk assessments to identify and evaluate compliance risks and controls for detecting breaches with relevant laws, regulations and significant corporate policies, including with respect to proposed new products or services or significant variations of existing products and services.
- Developing and implementing appropriate compliance training and team member and directors awareness programmes.
- Providing guidance to business units on the applicability of laws, rules and regulations to new products.
- Reviewing clients requiring EDD, including those classified as High Risk.
- Conducting routine and targeted compliance testing of the business units' related AML procedures and of other key units with AML responsibilities.
- Identifying, monitoring, and investigating any potentially suspicious activity identified by monitoring systems and referred by business units, and making the appropriate reports to the Designated Authority.
- Conducting investigation and verification of information for clients requiring EDD.

- Conducting initial client due diligence checks (i.e., OFAC, PEP[1] and adverse searches), maintaining evidence of such checks.

3.6 GROUP CHIEF COMPLIANCE OFFICER

The Group Chief Compliance Officer is responsible for overseeing and managing the AML Programme. The Group Compliance Manager is the Nominated Officer based on the Proceeds of Crime Act. All references to the Nominated Officer in this document should be interpreted to mean the Group Chief Compliance Officer or designated Country Compliance Officer.

The Group Chief Compliance Officer is supported by the Compliance Team which is comprised of a Country Compliance Officer, the Senior Compliance Manager, Compliance Analysts and a Legal and Regulatory Officer. The Group Chief Compliance Officer responsibilities include:

1. Being fully acquainted with the provisions of the Proceeds of Crime Act (as amended). He/she must, in particular, be cognizant of the confidentiality requirements with regard to reporting transactions.
2. Remaining informed of the local and international developments in money laundering and industry best practices.
3. The training of all team members with respect to the AML & CFT programme and the applicable regulatory and legal requirements.
4. Ensuring that all the companies within JMMB comply with the appropriate standards and procedures in place for AML & CFT Compliance.

[1] PEP generally includes current or former senior foreign political officials, their immediate family, and their close associates.

5. Ensuring that all team members are kept up to date on current legislative requirements both locally and internationally.
6. Establishing a compliance plan which will include independent review and on-going testing of team members' compliance in order to achieve the KYE requirements.
7. Implementing programmes, policies, procedures and controls to detect money laundering and terrorist financing activities.
8. Establishing a reporting system whereby team members can report activities which are not in compliance with JMMB's policies without fear of reprisal.
9. Establishing and publicizing a reporting system whereby other employees and agents can report criminal conduct by others within the company without fear of retribution.
10. Producing reports on matters of compliance to the Board of Directors of each entity and the Executive Team on the effectiveness of the AML/CFT framework. An annual comprehensive compliance report is done to JMMB Group Limited and JMMB Bank (Jamaica) Limited's Board of Directors
11. Evaluating reports of suspicious/unusual transactions by personnel and ensuring that reports for Threshold, Suspicious Activity and Suspicious Transactions are submitted to the FID in a timely manner.
12. Evaluating reports of Suspicious or Unusual Transactions and verify whether they are subject to reporting.
13. Ensuring that Compliance Analysts keep abreast of the changing regulatory and AML environment by attending the requisite training courses on an annual basis.
14. Acting as liaison between JMMB and regulatory and law enforcement agencies with respect to all compliance matters and investigations.
15. Ensuring that all exceptions are addressed and follow-up to ensure that corrective action is immediately instituted.
16. Ensuring that adequate resources are in place to effectively monitor compliance.
17. Evaluating new products and services to determine the level of risk and make appropriate recommendations.

18. Liaising with JMMB's legal counsel on AML matters and investigations.
19. Ensuring risk assessments are done by JMMB; and overseeing the risk assessments done by JMMB to ensure the appropriate risk profiles are established and the relevant measures and mechanisms commensurate with the risks assessed, are implemented; and ensuring these assessments are kept up to date and relevant
20. Coordinating with the JMMB's audit, legal and security departments on AML/CFT matters and investigations; and on matters pertaining to targeted financial sanctions notified by the United Nations Security Council
21. Overseeing administrative matters related to Code of Conduct and Compliance with Anti-money Laundering and Terrorist Financing Activities

3.7 ALL TEAM MEMBERS

Team members should be aware, of and comply with, requirements regarding compliance with the AML Programme, the JMMB Code of Ethics and the internal polices of JMMB. Any Team member who suspects or learns that a transaction or account is unusual must promptly notify the Compliance Department by completing an UTR. The Compliance Department will take steps to investigate, close or otherwise restrict the account and consider whether a STR should be filed.

All team members of JMMB have the primary responsibility for the relationship with the client and are ultimately responsible for forming a reasonable belief that JMMB knows the true identity of a client and can reasonably establish expected and usual activity.
The team member's responsibilities with regard to KYC are as follows:

- Interacting with a client to obtain all required KYC information and documentation prior to account opening as well as interacting with a client to update any KYC

information or documentation as part of on-going reviews/updates. This includes identifying any US indicia for the purposes of FATCA.

- Interacting with the client to ensure clients understand the Client Information verification requirements and other KYC requirements outlined in the KYC Policy (see section on KYC Policy).
- Forming a reasonable belief that the team member knows the true identity of each client based on the requisite due diligence and communicating this by signing-off on the completed Client Information Form or Client Update Form to confirm the accuracy and completeness of the client file.
- Maintaining vigilance in the normal course of business to identify and escalate unusual or suspicious activity as required by JMMB's suspicious activity escalation procedures. (Each Branch Manager and Head of Department is designated as the Compliance Officer for his/her branch/department and as such has the responsibility to ensure that matters are appropriately escalated to the Group Compliance Manager).
- Participating in updating client's KYC file and periodically confirming that a client's information and risk rating is accurate and up-to-date.
- Participating in targeted KYC training and AML training.

The Branch Managers (BMs), Branch Operations Managers (BOMs), Client Relationship Managers (CRMs), Personal Portfolio Managers (PPMs) and their respective Team Leaders support the Compliance Department by obtaining, reviewing and confirming the completeness of KYC information and the quality of the documentation gathered during the client acceptance process and throughout the duration of the relationship with the client. Their responsibilities with regards to KYC also include:

- Reviewing and signing-off on the completed KYC file, including approval of any change in the client information.
- Forwarding KYC-related documents to the Compliance Department for further

analysis when appropriate.

- Maintaining vigilance in the normal course of business to identify and escalate unusual or suspicious activity.
- Seeking the guidance of the Compliance team members on matters that relate to AML / POCA etc.

All client-facing team members must know who their clients are, their business and what can be deemed an unusual transaction for the client. KYC is beyond what is required by law but more about truly knowing the client to identify changes in their business-related behaviour.

4 SECTION I: ANTI-MONEY LAUNDERING & COUNTER FINANCING OF TERRORISM

4.1 DEFINITIONS

4.1.1 Definition of Money Laundering

Money laundering may be defined as:

- The process and transactions conducted to make illegally acquired money look as if it were acquired legally,
- The handling of money in such a fashion as to conceal its true source of origin
- The process by which income of illegal origin is transformed into money which appears to have been legitimately earned or obtained

The Stages of Money Laundering

The three basic stages by which criminals attempt to launder money are:

1. **Placement:** Placing unlawful money into a financial and/or non-financial institution

2. **Layering**: Separation of unlawful money from the original source, through the use of layers of financial transactions. Layering would include such actions as transferring the principal sum into multiple smaller amounts, which are then converted into traveller's cheques, money orders or other valuable assets (jewellery, art and paintings etc.)

3. **Integration:** Using apparently legitimate transactions to disguise unlawful cash.

Financial Institutions, as providers of a wide range of services, are vulnerable to being used at all stages but are primarily used in the layering and integration stages.

It should be emphasized that there are also many crimes (particularly the more sophisticated ones) where cash is not involved; securities, mortgage and other loan accounts may be used as part of this process to create complex layers of transactions

4.1.2 Definition of Terrorist Financing

Financing of terrorism is a term used to describe the accommodating or facilitating of financial transactions that may be directly or indirectly related to terrorists, terrorist activities and/or terrorist organizations. In some cases, proceeds from criminal activities are used in funding terrorist organizations or activities. It should also be noted that terrorist funding may be generated from legal sources.

4.2 COMPLIANCE MONITORING AND TESTING

4.2.1 Team member Monitoring of Transactions and Account Activity

1) Team members who manage the client relationship or accept and process client transactions are the **first line of defence** in understanding the normal and expected activity of a client and are therefore in the best position to monitor transactions.

2) **All team members must be vigilant in identifying changes in client transactions that appear inconsistent with the expected transaction type and activity level for the client.** Where such change in activity level is identified, the team member must communicate with the client and obtain up to date information including any expected change in profile or activity levels. Such information should be documented and filed. If the team member believes the particular transaction or trend is unusual based on the understanding of the client, such transaction should be reported immediately to the Compliance Department.

3) Compliance Analysts must also be vigilant in identifying changes in client transaction or activity trends and seek additional information from frontline team members.

4) Where outstanding information is identified in relation to particular clients, these should be requested from the designated frontline team members where applicable.

4.2.2 Compliance Department Monitoring, Review and Testing

In relation to the monitoring of transactions, the Compliance Department is responsible for the following:

1) Daily monitoring of transactions and performing historical analysis of client accounts or transactions where necessary.

2) Ensuring the names of new and existing clients maintaining accounts with JMMB are automatically compared to the most recent OFAC List. A report is generated on a

weekly basis which must be reviewed to determine whether further investigations are required for any client names identified or whether a suspicious transaction report should be filed.

3) Reviewing potential high-risk clients before a relationship is established except for non-resident whose reviews are done by the Branch Manager or their designate.

4) Updating the internal Watch List on an ongoing basis.

5) Working closely with the regulators and keeping abreast of international media in order to identify persons associated with illegal activity, Non-Cooperative countries, countries with weak AML/CFT frameworks and individuals and organizations associated with terrorism.

6) Adopting a consolidated approach in the assessment of clients with multiple accounts within JMMB. These are to be reviewed periodically.

7) Conducting compliance testing of aspects of the AML/CFT Programme at each Branch at least on an annual basis.
8) Conducting due diligence and EDD on clients, including prospects.

4.2.3 Independent Audit

1) The internal auditors will conduct a review at least annually of the AML Compliance Framework and determine the effectiveness of the compliance programme in place. This review will incorporate at a minimum:

a. an assessment of the duties and responsibilities of the Compliance team members
b. adequacy of the AML/CFT Policies and Procedures
c. AML/CFT Training Programme
d. integrity and reliability of the systems used for AML/CFT compliance

e. selection of accounts on a sample basis to ensure adherence to policies and procedures and the regulations and guidance notes issued by the regulators

2) An audit should involve the conduct of interviews with team members who handle transactions, the team leaders, and the designated anti-money laundering officers, including the 'Appropriate Person'.

3) Findings and recommendations of the audit should be communicated to the Audit Committee of the Board of Directors, Compliance Department, Executive Team Leaders, Senior Management, the Competent Authority, and as well as any other relevant individuals or departments.

4) JMMB may request that an independent audit of the AML Compliance Programme be conducted by the internal auditors to assess its effectiveness.

4.3 THRESHOLD TRANSACTIONS

The POCA requires each financial institution to file a report with the Designated Authority in relation to any cash transaction involving the prescribed amount. The prescribed amount is referred to as a threshold transaction and varies based on the type of financial transaction.

4.3.1 What are Threshold Transactions?

Threshold transactions relate to all cash transactions (deposits, investments, withdrawals, encashments or purchase or sale of foreign currency):

- For investments, encashments, deposits or withdrawals greater than or equal to US$15,000 or its equivalent in Jamaican currency or any other foreign currency.
- For cambios greater than or equal to US$8,000 or its equivalent in Jamaican currency or any other foreign currency.

- For remittance greater than or equal to US$5,000 or its equivalent in Jamaican currency or any other foreign currency.

4.3.2 Structured Transactions

1) A person may conduct multiple cash transactions in the same or different currencies within the same day and each transaction may not individually exceed the threshold amount but would equate to or exceed the threshold amount when they are accumulated. In these instances, all the transactions that collectively equate to, or exceed the threshold amount on the particular day should be reported on the threshold transaction form.

2) Transaction trends which indicate that each transaction amount consistently falls just below the threshold limits and for which no justifiable reasons can be obtained should be reported as suspicious transactions.

4.3.3 Cambio Transactions

Clients doing cambio transactions are required to provide JMMB with the KYC information and copy documents (including ID information) required by this policy, except in the cases where this information is already on file for them

If information is not on file, it is the responsibility of the team member processing the transaction to ensure that copies of relevant documents are received and JMMB records (electronic and paper) are updated. Identification tendered must be scanned to Universal Client Services (UCS) and copied. The ID must be valid and picture shown must bear resemblance to the actual person. The photocopies should be retained with the client records.

Identification is required, as stated in the policy, for all cambio transactions in excess of US$250.00 (de minimis amount) or the equivalent in any other currency. However, all other AML/CFT precautions and requirements remain applicable. The de minimis KYC

exemption is not applicable to transactions that require disclosure under sections 94 and 95 of the POCA, that is, where the transaction is deemed suspicious.

For any cambio transaction above US$1,000.00 or its equivalent in any other currency, the source of funds must be ascertained. A Source of Funds form must be completed along with supporting documents, where applicable, and saved to the source of funds folder on the o/public server for the respective branch for any transaction amounting to or exceeding US$8,000.00 or its equivalent in any other currency.

Where a transaction appears to be suspicious the transaction should not be conducted. The suspicious transaction must be immediately reported to the Compliance Department via a UTR.

4.3.4 Remittance Transactions

Verification of Identity for Remittance Customers

The customer profile for JMMB Money Transfer (JMMB MT) falls into the following categories:

- Customers conducting one-off transactions
- Repeat customers – defined by the Guidelines as "persons who do business with a primary agent more than once in any three (3) month period, irrespective of the amount". This applies to both inbound and outbound transactions.

For any transaction above US$500.00, or the equivalent amount in any other currency, valid identification must be obtained for individuals and corporate clients. Documents must be copied, signed and maintained on file by the agents.

Minimum Information Required for both Inbound and Outbound Transfers

The clients (beneficiaries/receivers and senders for outbound transactions) of JMMB MT must

complete a "Receive Money Form" or a "Send Money Form" and provide the following information:

- Valid Identification (Driver's Licence, Passport, National ID)
- Full name and any other names used (aliases)
- Correct permanent address
- Date and place of birth
- Telephone number (work, home, cell)
- Taxpayer Registration Number (TRN) or any other Reference Number

Customer Verification for Outbound Transactions

JMMB MT agents, when executing outbound transactions, must ensure that in addition to the minimum information required above, the following information on the sender is obtained for all outbound transactions:

- Valid identification which must be copied and retained
- Source of Funds for all transactions.
- Occupation
- Documents verifying source of funds may be required for amounts exceeding US$1,000 or its equivalent in any other currency.

Other Acceptable Forms of Identification

Other acceptable forms of identification for JMMB MT clients are:

· Employee ID with a photo from a well-known employer in addition to the TRN

· A birth certificate for the individual along with a Declaration of Identification and a photograph signed by a Justice of the Peace, Minister of Religion or an Attorney-at-Law confirming the identity of the person.

· A valid school ID, where the student is enrolled in a secondary or tertiary institution. The

ID must have the following features:

- A photograph of the student
- Signature of the student
- ID number
- Expiry date
- Name of the school or tertiary institution
- Signature of the principal/bursar/vice-principal

Discontinuing a Relationship with a Remittance Customer

JMMB MT reserves the right to refuse to process a transaction for a client or terminate a relationship with a repeat client if the transaction or transactions appear(s) suspicious or is/are not in accordance with regulations. A relationship with a repeat client may also be discontinued if such customer represents a significant reputational risk to JMMB MT or any other member of the JMMB Group.

Repeat Remittance Customers

- Where a remittance client conducts transactions more than once, JMMB MT may require such clients to provide full KYC information.
- Repeat clients should be clearly identified on the system to enable monitoring and assessment where required.
- Identification documentation must also be photocopied and filed by JMMB MT.

Verification of Potential Remittance Partners and Agents

- **Potential Partners**

All potential partners will be required to complete the Due Diligence Check List for the Remittance business and to provide certain minimum information before the potential alliance

is approved (See Appendix for copy of Checklist). This includes information on the beneficial owners, the group structure and the regulatory framework within which the potential alliance operates. Evidence of the requisite licence and approvals and management expertise and track record are also required where applicable.

- **Agents**

All clients approved as agents for JMMB MT must be approved by the BOJ before being accepted as agents of JMMB MT. Agents will be required to complete and provide all documents required by the BOJ and authorised by the Chief Executive Officer of JMMB MT before submission to BOJ.

5 REPORTING TO THE DESIGNATED AUTHORITY (THE FID)

1) A Nominated Officer is designated for each entity based on the POCA and is the primary liaison person between JMMB and the Designated Authority.

2) All reporting to the Designated Authority (Chief Technical Director, FID) must be done through the respective Nominated Officer or their designate.

3) The Compliance Department is required to file all threshold transaction reports within fifteen (15) days of the end of each month to the CTD, FID.

4) The Compliance Department must track all threshold transactions and ensure the accurate submission of the threshold transaction report. Separate threshold transaction reports must be submitted for each regulated entity within the JMMB Group.

5) A NIL Threshold Transaction Report must be submitted if there are no threshold transactions for the reporting period.

5.1.1 Consequence of Failure to Submit Threshold Reports

Failure to submit reports within the stipulated deadline may result in a fine not exceeding Four Hundred Thousand Dollars (J$400,000) being levied against JMMB as well as the Officer responsible for ensuring that reports are submitted to the Group Compliance Officer/CCO.

5.1.2 Exemptions from Threshold Reporting Requirement

Transactions involving any of the persons listed below may be exempt from the threshold reporting requirement. ***They are not, however, exempt from the suspicious transaction reporting regime:***

- A ministry, department or agency of government
- A statutory body or authority
- A company registered under the Companies Act in which the Government or an agency of Government is in a position to influence the policy of the company by virtue of its shareholding or other financial input
- Any Embassy, High Commission, consular office or organization to which the Diplomatic Immunities and Privileges Act applies.
- Any organization in relation to which an order is made under the Technical Assistance (Immunities and Privileges) Act

The Designated Authority reserves the right to request information from the financial institution on the following entities exempt under the TTR regime:

- A ministry, department or agency of government;

- A statutory body or authority; or
- A government company.

It is the policy of JMMB not to apply for exemption from Threshold Reporting for any retail or corporate client.

5.2 SUSPICIOUS TRANSACTIONS

5.2.1 What is a Suspicious Transaction?

It is difficult to determine what a suspicious transaction is without having a good understanding of the client and the client's normal expected activities in order to recognize that a transaction or series of transactions is unusual. A transaction may be considered to be suspicious if:

- It is complex, large, unusual or inconsistent with the client's normal transactions or patterns of transactions. (The transaction may be deemed suspicious whether it is completed or not); or

- The transaction does not appear to have any business or apparent lawful purpose based on initial and subsequent interviews with the client.

- Based on its size, however, any transaction or pattern of transactions, irrespective of the amount of the frequency, may be deemed suspicious. Examples of activities that may give rise to suspicion are provided in Appendix II of this manual.

5.2.2 Suspicious Transactions are Prohibited

A transaction that appears to be suspicious should not be executed unless consent is obtained from the Group Chief Compliance Officer or designate. The decision on whether the transaction should be processed should be based on the nature of the transaction, the relationship with the client and the information and documentation provided or available.

No potential client relationship should commence or business arrangement undertaken if the client, transaction or arrangement is deemed suspicious.

5.2.3 Exceptions for Suspicious Transactions

Suspicious transactions may only be undertaken if the Country Compliance Officer or designate gives consent and immediately reports such transaction to the Designated Authority.

Suspicious transactions may also be undertaken if the Country Compliance Officer or designate obtains appropriate consent from the CTD or an appropriate officer from the FID before the transaction is executed.

5.2.4 Internal Reporting of Suspicious Transactions

1) Suspicious transactions may be identified by any team member involved directly or indirectly in the processing of client transactions.

2) Transactions in relation to new or existing accounts that are deemed suspicious should be communicated immediately to the Compliance Department.

3) The Country Compliance Officer is to be immediately notified (before the transaction is processed) when a transaction is presented that appears suspicious. The Country Compliance Officer must assess the team member's findings and make a determination on whether the transaction should be reported suspicious.

5.2.5 Reporting Suspicious Transactions to the FID

All STRs to the Designated Authority must be made by the Compliance Department. Reports are to be filed as soon as possible and no later than fifteen days (15) days after an attempt is made to conduct what appears to be a suspicious transaction or as soon as possible after the transaction has taken place.

5.2.6 Terminating Relationships Due To Continued Suspicious Activity

The Compliance Department may recommend the termination of a client relationship if it is deemed that the activity on the account is suspicious and the relationship, if continued, may affect JMMB's correspondent relationships or expose it to significant regulatory or reputational risk. Where this is done a report will be made to the FID.

5.2.7 Treatment of Suspicious Transactions Detected During the Account Opening Process

If a suspicious transaction is identified before a relationship is established, the person conducting the transaction should obtain, at a minimum, the identification information before refusal of service is communicated to the potential client. The attempted suspicious transaction must be reported to the Compliance Department.

Transactions that do not appear to be suspicious but raise questions should be reported via a UTR for closer scrutiny by the Compliance Department, if the relationship is established.

5.3 UNUSUAL TRANSACTIONS

Each entity within the Group will be required to document and keep information on all complex, unusual or large transactions by way of an UTR which should be available upon request to the FID. This information should be kept for a period of not less than seven (7) years.

5.4 REPORTING TO THE BOARD OR AUDIT COMMITTEE

Reports by the GCCO or CCO are to be submitted to the Board of Directors or the Audit Committee at least quarterly. The following is a list of items that should be included in the report:

a. Any changes made or recommended in respect of new legislation;
b. Serious compliance deficiencies that have been identified relating to current policies and procedures, indicating the seriousness of the issues and either the action taken or recommendations for change;
c. A risk assessment of any new types of products and services or any new channels for distributing them and the AML and CFT compliance measures that have either been implemented or are recommended;
d. The means by which the effectiveness of ongoing procedures have been tested;
e. The number of internal reports that has been received from each department, subsidiary, etc.;
f. The percentage of those reports submitted to the designated authority;
g. Any perceived deficiencies in the reporting procedures and any changes implemented or recommended;
h. Information identifying team members trained during the period, the method of training and any significant issues arising out of the training;
i. Any recommendations concerning resource requirements to ensure effective compliance.

6 CLIENT FILES

A static data file should be maintained for all clients. Such files will include the following minimum information:

a. Completed account opening documents signed by the client

b. Certified copies of incorporation documentation and records of client identification (KYC documents)
c. Any other information, including client instructions and client correspondence for each client

JMMB will also be required not only to update each client's information every seven (7) years, but also to keep the client's information under constant review with a view to ensuring its accuracy.

6.1.1 Transaction Records

a. Records of all transactions undertaken during the course of a client relationship will be retained in the form of original documents, copies of original documents, and electronic data. Each document retained should provide information on the date and nature of the transaction, the amount and type of currency used (where applicable) and the client account(s) affected by the transactions. Each record should provide sufficient information to ensure that a satisfactory audit trail exists.

b. Transaction and client identification records will be maintained for a period of at least seven (7) years after the date the relationship has been terminated or the last transaction.

6.1.2 Records of Threshold, Unusual and Suspicious Transactions to the Financial Investigation Division

a) JMMB shall maintain a Register of Reports. The Register will cover UTRs, STRs and TTRs. The Register of Reports will be managed by the Senior Manager, Compliance.
b) Reports made by team members, UTRs, are to be sent in a sealed envelope directly to the Country Compliance Officer or Senior Manager, Compliance.
c) The Register of UTRs should contain the following information:

i. The date of the report
ii. The team member who made the report
iii. The signature of the reporting team member
iv. The nature of the report
v. A reference by which any supporting document is identifiable
vi. The reason for not submitting a report to the Designated Authority (where applicable)
vii. Date of receipt of acknowledgement (for reports submitted to the Designated Authority)

d) Records of TTRs and STRs submitted to the FID will be retained for a period of at least seven (7) years commencing on the date the report was filed.

e) Reports and transactions relating to on-going investigations should be retained until confirmation is received (in writing) from the FID that the case has been concluded and that further retention is unnecessary.

6.2 ENFORCEMENT AND INVESTIGATIONS

1) JMMB may be required to provide information, monitor accounts or perform certain activities based on Court Orders. These Orders may include Forfeiture, Pecuniary, Penalty, Restraint, Disclosure and Account Monitoring, Search and Seizure and Client Information Warrants. These enforcement and investigatory Orders may be served on JMMB and the response, based on the order, in relation to client relationships that are maintained or were maintained with any entity within JMMB would be required.

2) The Compliance Department must ensure that the appropriate responses are provided to these requests, noting the stipulated deadline. Consultations should be made with External Legal Counsel where necessary, in responding to these Orders.

3) Any request of this nature received by any other Department within JMMB should be forwarded to the Compliance Department, and the team member forwarding the information should maintain the confidentiality standards needed for compliance with POCA.

4) The CTD or such other appropriate officer may apply to the court for an "Account Monitoring Order" directing JMMB to disclose information within the period specified in the order (not exceeding ninety days) or provide material on the account specified in the order or regarding a transaction conducted, also specified in the order.

6.2.1 Account Monitoring Orders

1) Where "Account Monitoring Orders" are issued by the CTD and are in place, this should not be disclosed to any person except:
    a) An attorney, for the sole purpose of seeking legal advice or representation in relation to the Order; or
    b) An officer or agent of the institution, solely for the purpose of ensuring that the Order is complied with.

6.2.2 Client Information Order

1) The CTD or such other appropriate officer may also apply to the Court for a "Client Information Order". This Order is for information on whether a person holds/held (solely or jointly) any account with a financial institution or has conducted a transaction with a financial institution. The particular information required by the Client Information Order is as follows:

    a. Account/transaction number
    b. Full name and date of birth
    c. TRN

d. Most recent address and previous addresses
e. Date on which the individual began to hold and/or ceased to hold the account
f. Transaction date and description of transaction type
g. Proof of identity obtained by the financial institution
h. Full name, date of birth, most recent and previous address of any joint holder of the account.
i. Account number of any other accounts to which the individual is a signatory and details of the persons holding those accounts.

In the case of non-individuals the following is required:

a. Account number
b. Entity's full name
c. Description of the business carried on by the entity
d. Country or jurisdiction of incorporation or establishment
e. TRN
f. Registered office or place of business (in or outside of Jamaica)
g. Date on which the entity ceased to hold the account
h. Evidence of the entity's identity obtained by the financial institution
i. Full name, date of birth, most recent and previous addresses of any person who is a signatory to the account.

This order does not have to be specific to JMMB and may speak to all financial institutions or a particular type of financial institution.

6.2.3 Asset Recovery

The passage of the Proceeds of Crime Act (POCA) 2007 has increased the responsibilities of the FID and has provided an increase in investigative and asset recovery powers as well as the

establishment of compliance responsibilities for financial institutions and certain non-financial institutions. It established the Asset Recovery Agency which is charged with the responsibility of seizing and forfeiting assets that are unlawfully obtained thereby removing the profit out of crime. The Asset Recovery Agency has twenty (20) years within which to commence proceedings for a Recovery Order under Section 58 of the Act.

6.3 TEAM MEMBER ACCOUNTABILITY

6.3.1 Team Member Integrity

JMMB is cognizant of the risks attached to having inadequate systems to deal with e.g. dishonest team members because the success of the AML and CFT programme depends to a large extent on the integrity of team members. JMMB has established and implemented appropriate policies and procedures to ensure that team members are "fit and proper" persons.

To this end, potential team members are subjected to a comprehensive screening process, which involves a thorough investigation of the potential team member's background, honesty, competence and integrity.

JMMB has also instituted processes geared towards ensuring the continued maintenance of a high level of integrity and competence among team members. This includes but is not limited to: -

1. Establishment of a Code of Ethics which shall govern the conduct of all team members
2. Regular review of team member performance and adherence to internal policies and procedures including codes of conduct and AML/CFT requirements;
3. Imposition of appropriate disciplinary sanctions for breaches of the institution's AML and CFT policies;
4. Close scrutiny and investigation of team members whose lifestyles cannot be supported by

his or her known income;

5. Review of team members' accounts; and
6. Investigate team members' involvement in suspected fraudulent activities.

It is the responsibility of the Culture and Human Development Team of JMMB to perform the following due diligence procedures when hiring new team members:

a. Personal background checks;
b. Previous employment checks;
c. Verification of financial history;
d. Verification of professional qualifications;
e. Obtaining a declaration of assets;

In doing so:

1) At least two (2) written references are required, one of which must be from the previous employer (where applicable)
2) The reason for termination, where applicable, needs to be stated in the previous employer's reference.
3) Periods of unemployment should also be explained and substantiated by written references.
4) Referees must be in a position to attest to the character of applicants and must not be relatives or personal friends. There should be some formal basis for the applicant's relationship with the referee e.g. the applicant's pastor, banker, teacher, former co-worker, business client, Member of Parliament etc.
5) The financial history of the applicant should be established as follows;
    a) Examination of the two most recent statements from each of his/her bank accounts.
    b) The applicant may also be asked to provide information on his credit history. A letter from each bank could establish this.
    c) The real estate holdings of the applicant may be requested as well as any other assets and liabilities. This may be established by way of a standard balance sheet. For

example, in order to monitor changes to the holdings, employees may be required to submit annual statements of affairs, thereafter.

d) JMMB must seek an explanation for any unusual ownership in assets not supported by the applicant's earning history.

For existing team members the Culture and Human Development Team (CHDT) of JMMB must:

1. Where necessary, obtain clarification and/or explanation for significant changes in the lifestyle of a team member (especially where it appears that his/her salary cannot support such lifestyle);
2. Review of debt obligations at least annually by the Credit and Human Resources designated officers
3. Ensure that team members take their prescribed vacation leave.
4. Ensure that team members uphold the culture and values of JMMB.

6.3.2 Know Your Employee (KYE)

The reputation and operations of any institution rest heavily on the integrity, quality and efficiency of its team members.

All team members must be guided by the Code of Ethics/Conduct, which all team members must read and sign at the beginning of their employment with JMMB.

Team members' accounts should be operated according to the guidelines set out in the "Operating Guidelines for Team Members of Financial Institutions".

Activity on all team members' accounts will be monitored by the Compliance Department.

The following KYE reviews for team members may be necessary under the following circumstances: -

- Upon the execution of a significant staff transaction;
- When there is material change in the manner in which their staff account is being operated;
- When, during the course of the business relationship, doubt arises regarding the true identity of the beneficial owner of the account tagged as staff;
- Where transactions carried out in a single operation or in several operations appear to be linked; and
- Ascertain team member's citizenship status for FATCA purposes

6.3.3 Training

All team members of JMMB are required to be trained at least annually on this policy and procedure. New team members and directors are trained during the orientation session.

Training initiatives can be done via any of the following:

1. Scheduled live sessions
2. Videotaped presentations
3. Intranet learning applications
4. Online training and assessment

Each team member will be tested on the material and a pass rate of 80% must be achieved before certification is received.

Where team members do not achieve the required 80% pass rate, a special training session will be held for such team members; they will be required to retake the assessment after the special training session.

6.3.4 Training Programme for JMMB Team members

The effectiveness of the policies contained herein to a large extent will depend upon each team member's understanding of the impact of money laundering and terrorist financing on our day-today business activities. As a result:

a. All team members must be aware of their personal obligation under the Proceeds of Crime Act and the Regulations and the policies and procedures detailed in this policy document.

b. All team members should understand their obligation and responsibilities under the Code of Conduct, the Anti-Money Laundering Policy Manual and the reporting channels for suspicious or unusual activities.

c. All new team members of JMMB, regardless of their level or seniority, must receive training in Anti Money Laundering and Counter Financing of Terrorism during their orientation period. Training will address the following areas:

- The policies and procedures in place to detect and prevent money laundering and terrorist financing.
- The basic elements of the Proceeds of Crime Act, The Proceeds of Crime (Money Laundering Prevention) Regulations, the BOJ Guidelines, the FSC Guidelines, & FATCA.
- The sanctions for non-compliance under these laws & Guidelines.
- The background to money laundering and the international initiatives

driving the changes, including the Basel Committee, the Financial Action Task Force (FATF), the Caribbean Financial Action Task Force (CFATF), the US Patriot Act and USA Kingpin Act.

- The obligations of the team members and JMMB under the relevant laws, with an emphasis on the legal obligation of each team member.

- The recognition and handling of suspicious or unusual transactions

- An explanation of the legal obligations of both the team member and the employer under the current Anti-Money Laundering and Counter Terrorist Financing Laws and Guidelines
- Current and emerging money laundering and terrorist financing methods, trends and best practises

- JMMB s' "Know Your Client" Policies and Procedures.

d. **ALL** team members must be aware of their own personal obligations, as they can be held liable for failure to report suspicious or unusual transactions to the Compliance Department.

6.3.5 Annual Training for All Team members and Directors

Refresher courses will be conducted annually or at other intervals considered necessary. This is to ensure that all team members are aware and understand the policies of JMMB and the importance of compliance with the Anti-Money Laundering and Counter Terrorist Financing Regulations and their responsibilities and obligations under the relevant laws. Evidence of this training will be documented and filed.

6.3.6 Training Methods

Training will take the form of formal presentations by external or in-house experts or external courses conducted by reputable and competent institutions. Team members will also be provided with relevant materials through the intranet to enhance awareness of compliance issues and to communicate updates in the regulations or guidance notes issued by the regulators.

6.3.7 Records of Training

Training records should be maintained which detail the following information:

a. The details of the course material and the targeted level of team members

b. The names and signature (electronic or ink) of all team members in attendance and the date the training course was delivered

c. The name of the presenter and completed evaluation form.

The results of any test taken by team members to assess their understanding of AML requirements in relation to the training course

6.3.8 Wilful Blindness by Team Members

Wilful blindness occurs when a team member ignores facts which a reasonable person would consider suspicious. A team member does not have to be actively involved in assisting money laundering in order to be held legally liable for the crime of money laundering. To the contrary, a team member who had the knowledge or should have known that funds were tainted or who failed to investigate red flags for suspicious activity, and still completes a transaction involving such funds, may be liable for money laundering. Even where there is no direct evidence of an

individual's knowledge concerning tainted funds, that individual may be found to have been wilfully blind or to have acted with reckless disregard for the facts, and therefore be liable.

6.3.9 Prohibited Team Member Actions

Team members should not:

1) Knowingly, or with wilful blindness, provide advice or other assistance to clients or anyone doing business with JMMB, who wish to violate/avoid AML laws or provisions of the AML Programme;

2) Knowingly, or with wilful blindness, permit clients or anyone doing business with JMMB to execute transactions in such a manner so as to break or obscure the audit trail.

3) Conceal a suspicious or unusual transaction; or advise a client that information relating to the client is being reported as suspicious or unusual (in a STR or UTR or any other medium). Advising a client that a STR or UTR is being filed with the FID is an offence under the POCA.

4) Advising a client on how to avoid FATCA reporting.

6.3.10 Sanctions in Relation to Non-Compliance

1) Sanctions for non-compliance with all policies, procedures and practices range from verbal warnings to termination of employment. Additionally, non-compliance with the POCA may be criminal offence for which a team member may be held accountable.

2) Each team member is responsible for protecting JMMB from being used by money launderers. Involvement with money laundering activity, even if unintentional or indirect, *e.g.*, through an association with a client or other persons that are involved in such activities, could also cause significant and long-term harm to the reputation of JMMB.

3) JMMB will take all necessary steps to prevent its products, services and facilities from being used to launder funds derived from illegal activities.

4) Team members must therefore comply with the applicable AML laws and regulations as well as regulatory expectations, the provisions of this AML Programme, and the policies and procedures and internal controls that apply to his or her position and duties.

5) Failure to comply with applicable legal requirements or the AML Programme and JMMB-related policies and procedures will result in disciplinary action, including termination of employment. Individual team members may also be subject to criminal and civil penalties, including, but not limited to incarceration and monetary penalties, for failure to comply with AML laws and regulations. (See Appendix IV for fines and penalties for various offences).

6.3.11 Documents to be Signed by Team Members Annually

1) The JMMB Code of Conduct

2) AML, CFT & KYC Policy Statement

6.4 TEAM MEMBER INTEGRITY & AWARENESS

The Culture and Human Development Team is responsible for:

1) Obtaining and maintaining the requisite personal and financial history of team members. The information required is in accordance with best practices for the financial industry and ensures that team members meet the fit and proper standards required for their employment. This

information is also used in establishing the KYE Programme as required by the BOJ Guidelines.

2) Subjecting potential team members to a comprehensive screening process, which will involve from time to time:
    - A thorough investigation of the potential team member's background, honesty, competence and integrity
    - Reference checks
    - Checking the authenticity of academic qualifications

3) Establishing a Code of Ethics for all existing team members to guide team member's conduct.

4) Ensuring that the KYE programme is effective and in compliance with the regulatory guidelines and internal policies in collaboration with the Compliance Department.

5) Imposing the appropriate disciplinary action (including dismissal were appropriate) for breaches of JMMB s' AML/CFT and Know Your Client Policies and Procedures.

6) Ensuring that The JMMB Code of Ethics and Conduct is distributed to and signed by all team members annually.

Managers and Department Heads are responsible for:

1) Ensuring that their team members comply with the policies of JMMB. Where there is non-compliance which may result in disciplinary action, information must be communicated to the Culture and Human Development Team to ensure the applicable disciplinary action is applied.

2) Notifying the Culture and Human Development Team where there are indications of unusual changes in the team member's lifestyle and behaviour that may be difficult to substantiate.

6.5 TIPPING OFF

1) It is an offence for anyone who knows, suspects or has reasonable grounds to suspect that a report has been made, or that the CTD is acting or proposing to act in connection with an investigation into money laundering, to prejudice the investigation by so informing the person who is the subject of a suspicion, or any third party, of the report, action or proposed action.

2) Where it is known or suspected that a STR has already been made to the CTD and it becomes necessary to make further enquiries, great care should be taken to ensure that clients do not become aware that their names have been brought to the attention of the authorities.

6.6 CONFIDENTIALITY OF REPORTS

1) Reports submitted to the Financial Investigation Division (FID) and any other regulatory body whether local or international must remain confidential.

2) Reports filed for suspicious transactions with the FID should not be disclosed to any person or entity unless required pursuant on POCA

3) Team members should not disclose to any other team member, colleagues or clients (except the person to whom the transaction should be reported, or to the Country Compliance Officer and the Compliance Analysts):
    - that a STR, TTR or a UTR has been filed
    - that the transaction is or appears to be suspicious or unusual; or
    - that the transaction or the client is being investigated

4) Team members will not be held liable in relation to any criminal, civil or administrative liability, as the case may be, for breach of any restriction on disclosure imposed by contract or any legislative, regulatory or administrative provision if transactions are reported in accordance with this policy and confidentiality of the report is maintained.

5) A team member who makes unauthorised disclosures of any confidential reports in relation to suspicious, unusual or threshold transactions or any other such regulatory report is subject to disciplinary action, including dismissal, and may also be fined under the POCA.

7 SECTION II: KNOW YOUR CLIENT (KYC) POLICIES

"Know Your Client" Policies and Procedures are critical to the effective management of risks and the safety and soundness of the integrity of the system as a whole. KYC is closely associated with the fight against money laundering and the financing of terrorism, and is also an essential part of controlling and mitigating against reputational, operational, regulatory and legal risks to JMMB.

7.1 SCOPE AND PURPOSE OF KYC POLICIES

The KYC policies of JMMB will address four key elements of sound KYC standards:

- Client Identification and Verification
- Client Acceptance Policy
- Monitoring of Accounts
- Risk assessment of client relationships

JMMB has adopted a risk-based approach to the classification of its clients to ensure that the due diligence standards on clients are heightened in instances where client information indicates a higher susceptibility to money laundering risk.

These KYC Policies and Procedures are designed to foster a strong relationship with our clients, while taking all possible steps to protect JMMB's reputation.

With the introduction of FATCA, JMMB is required to ascertain whether any of its clients are US persons as defined by the FATCA regulations. Where a US person is identified additional scrutiny and, in some cases, reporting requirements will apply.

7.2 CLIENT IDENTIFICATION AND VERIFICATION

JMMB must at all times establish, to its satisfaction, that it is dealing with a real person (natural, corporate or legal). The identity of all persons conducting business with JMMB must be verified.

Proper identification of each client (including parties who may have a beneficial interest in the transaction or the account) and those that may be acting on their behalf (agents) must be ascertained before the commencement of any relationship.

Face-to-Face client interviews are to be conducted (in all cases where possible) to establish identity.

Before establishing a client relationship, verification of identity must be performed for all persons authorised to operate the account(s). This includes:

- Any persons or entities, corporate or unincorporated, who seek to establish a relationship.
- All partners/directors of a firm seeking to start a business relationship, who are relevant to the application and have individual authority to operate.
- Any person who is the beneficial owner of the account, namely any person who ultimately owns or controls a company.

- Any person who has a beneficial interest in the account or has direct or indirect control of the account.

7.3 RISK CLASSIFICATION OF CLIENTS

7.3.1 Risk Based Approach

JMMB has adopted a risk-based approach for the classification of all client relationships. The risk based approach to AML/CFT means that JMMB will implement the necessary mechanisms to identify, assess and understand the ML/TF risks to which it is exposed and take the requisite AML/CFT measures commensurate to those risks in order to mitigate them effectively and efficiently. It also takes into consideration the money laundering risk of each client and generally requires clients that are deemed to be of a higher money laundering risk to provide further information, in addition to the minimum information normally obtained for each client. There are certain businesses that have a higher risk of money laundering due to the nature of their activities and the lack of regulatory oversight by an independent body. The three categories for risk rating are high, medium or low with each having sub-categories. The factors listed in this policy are not exhaustive of all situations that may lead to a decision on the classification of the client. Therefore, sound judgment should be exercised where other factors not included in the list are present and should be taken into consideration. Note also that risk classification is done in conjunction with a client's income sources and projections.

JMMB shall identify, assess and take effective action to mitigate its money laundering and terrorist financing risks in relation to:

- customers and other counterparts;
- parties (i.e. persons other than customers with whom it conducts business);
- countries or geographic areas;
- products;
- services;

- transactions;
- delivery channels; and
- the operating environment (business size, activities and complexities);
- sector;
- national frameworks and national and global issues.

The assessment of risk (i.e. the Risk Based Framework) as itemized above shall be:

a. undertaken on an ongoing basis to take account of new risks and changing circumstances and must therefore be undertaken periodically (at least once per quarter or more frequently depending on the circumstances) and assessments must be documented;
b. undertaken so that there is a clear identification, determination and understanding of the risks involved;
c. based on practical, comprehensive and up-to-date understanding of threats;
d. approved by JMMB Group Board Committee responsible for the governance and oversight of JMMB, and made available to officers and employees or staff where commensurate with respective functions, to allow for the identified measures to be applied and monitoring to be undertaken; and
e. readily available to the internal and external auditors as well as the Competent Authority and Supervisory Authority.

7.3.2 Risk Assessment Requirements

1. All clients must be risk rated before a relationship is accepted or approved. The law defines "risk profile" as a formal assessment made by the regulated business concerned as to the level of money laundering risk posed to the regulated business

by the business relationship or transaction concerned.

2. All clients classified as high risk must also be approved by Senior Manager before the client account is established. The risk assessment process is used to determine the extent of due diligence for each client and the scope and frequency of monitoring of the client's account.

3. To determine the risk category of each client, the representative tasked with opening the account shall be take into account the following factors when assessing the money laundering risk associated with a client relationship:

    a. The nature of the client's business
    b. Whether the client is resident overseas
    c. The product or service that is being requested (wire transfers, foreign exchange transactions, cash secured loans, payable-through accounts, correspondent banking etc.)
    d. Geographic considerations (country of origin, principal place of business etc.)
    e. Source of funds
    f. The expected origin and destination of funds
    g. Method of account opening (non-face – to - face including internet, post etc.)
    h. Client profile (public official, high net worth, etc.)
    i. The client's political affiliation and level of association with a politically exposed person
    j. Verification of identification after the opening of the account
    k. Trust or Settlor Accounts
    l. Accounts opened by Professional Intermediaries on behalf of another
    m. Countries with inadequate AML/CFT/ Combating the proliferation of weapons of mass destruction frameworks
    n. Transactions via emerging technology e.g. Block chain, Crypto currency

Due to the relative nature of risk factors, the following should also be considered when performing risk assessments:

a. Clients in high-risk business activity may be legitimate clients.

b. The identification of one or more risk factors does not indicate that an illegal activity is taking place. Further enquiries should be conducted before any STR is raised.

c. The risk factors should be viewed mainly as indicators of the need for additional scrutiny. Many clients will have a mix of factors, some low-risk and some high- risk. In these circumstances, the risk category will be the higher of the two where there is no clear indication of the category in which the client falls.

7.3.3 Low-Risk Clients

Low risk individuals and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk. Examples of low risk customers may be salaried. A risk rating will be assigned based on the risk assessment model.

7.3.4 Medium-Risk Clients

Clients that are likely to pose a higher than average risk to JMMB may be categorized as **medium** depending on the client's background, nature and location of activity, country of origin, sources of funds and his client profile etc. A risk rating will be assigned based on the risk assessment model.

7.3.5 High-Risk Clients

High Risk clients are clients whose transactions are considered large or the nature and

structure of the business or profession make them more susceptible to being used for illicit activities. In conjunction with the risk rating assignment that will be done based on the risk assessment model, a detailed assessment of the following should be conducted:

i. Client's background
ii. Country of origin
iii. Profession
iv. Position (whether public or high-profile
v. Source of funds

Where a business relationship or one-off transaction is determined to be high-risk, JMMB shall carry out EDD measures which include but are not limited to:

i. Obtaining all relevant identification information that is required as per procedure prior to establishing the business relationship.
ii. Verifying identification information.
iii. Accessing publicly available information to assist in the determination as to whether or not the person is acceptable to JMMB
iv. Accessing, obtaining and verifying the source of funds and source of wealth to commence and maintain the business relationship
v. Conducting a face-to-face meeting with the prospective client to discuss / confirm the information given, purpose of account and source of assets.
vi. Assessing certain factors including customers' background, country of origin, important public or high profile position/(s) held, linked accounts, business activities or other risk indicators
vii. Seeking approval from senior management, excluding the Nominated Officer, to open the account
viii. If subsequent to the opening the account the risk profile changes to a higher level, approval must be sought from senior management to continue the business relationship

ix. Investigating to ascertain if the account holder has been refused banking facilities at another financial institution
x. Regular review of client records
xi. On-going monitoring of accounts

An annual review of all high risk accounts is to be conducted by the domicile branch. Compliance will conduct an annual sample review of all high risk clients. The report from the review will be shared with the General Manager, Client Partnership.

The following categories of clients should be classified as high risk due to the size of the transaction or the nature and complexity of the business or profession. Accordingly, all businesses that are classified as one of the following will receive increased scrutiny from the Branch Manager and Compliance Team Members.

The Compliance Department will review and determine whether or not JMMB will enter into a business relationship with the following high risk individuals, sectors or companies:

i. Politically Exposed Persons (PEPs) and immediate family members
ii. Remittance companies
iii. Cambios
iv. Gaming lounges and casinos
v. Liquor stores
vi. Land developers
vii. Cash-intensive businesses
viii. A person who is not ordinarily resident in Jamaica, if Branch Manager or designate is not available
ix. A person acting as a trustee for another in relation to the business relationship or one-off transaction concerned

x. Individuals who reside in jurisdictions / countries with inadequate AML/CFT Frameworks
xi. Trustees
xii. Off-shore corporations and companies located in tax havens
xiii. A company having nominee shareholders who are unknown or they nominee is unwilling to disclosed who are the beneficial owners
xiv. A member of such other class or category of person as the supervisory authority may specify by notice published in the Gazette

If the ultimate beneficiary/ies or beneficial shareholder/s cannot be reliably established or there are no reliable measures in place to monitor any changes in the ownership structure, the relationship should not be commenced, or where a business relationship has already been established, this relationship should be legally terminated.

JMMB will not establish business relationships with:

i. Foreign entities with bearer shares.
ii. Investment clubs (partner plans, pyramid schemes)
iii. Cheque cashing businesses
iv. Adult book stores
v. Adult entertainment clubs

7.4 PROHIBITED ACCOUNTS, RELATIONSHIPS AND TRANSACTIONS

JMMB prohibits wire transfers to any country on the OFAC/ UN list of sanctioned countries (see list in section 10).

JMMB will not conduct business with clients or execute any transaction where the following apply:

1) **Illegal Activities are suspected**: Clients whose information indicates possible involvement in illegal activities.
2) **Verification Not Possible**: Clients with businesses that make it impossible to verify the legitimacy of their activities or the source of funds.
3) **Refusal by the Client to Provide Required Information**: Clients who refuse to provide the required information or documentation.
4) **Entity is a Shell Bank**: Banks having no physical presence in the jurisdiction in which they are licensed to operate.
5) **Ownership Structure is via Bearer Shares-**: Bearer Shares are shares which are owned by the persons holding these shares. This allows ownership of shares to change easily and it may be difficult to determine the true beneficial owner.
6) **Nominee Shareholders are used:** Foreign entities having nominee shareholders and it is difficult to determine the ultimate beneficial owners.
7) **Anonymous or Fictitious Names are used**: Where clients wish to open anonymous accounts or accounts using fictitious names. JMMB will not open numbered/anonymous accounts or conduct transactions with persons by means of any such accounts.
8) **Entity is a Shell Company**: Legal entities that act as a "front" for illegal activities. It may be difficult to determine the true activity of such companies and therefore EDD procedures must be adopted where there are indications that entities have no business substance.
9) **Listed Persons or Entities:** Individuals and entities names appearing on the US treasury OFAC list or UN Sanctioned List.
10) **Suspicious or Unusual Transactions**: Where information obtained before or after processing a transaction is deemed suspicious or unusual.

8 PERMITTED PERSONS

The Proceeds of Crime (Amendment) Act, 2013 provides that only permitted persons will be authorized to pay or receive cash over JA$1M for the purchase of goods or services or for the payment or reduction of any indebtedness, account payable or other financial obligation.

A 'permitted person' includes a bank licensed under the Banking Services Act, a licensed deposit-taking institution regulated by Bank of Jamaica, a person licensed under the Bank of Jamaica Act to operate an exchange bureau or any other person that may be designated by the Minister as a 'permitted person' by Ministerial

Order.

Permitted persons may carry out cash transactions in excess of the cash transaction limit with any person.

Permitted persons must therefore not refuse to carry out cash transactions solely on the basis of a cash transaction exceeding the cash transaction limit. However, in facilitating cash transactions, permitted persons remain obliged to be reasonably sure that they do not facilitate a financial crime or other breaches of the law.

JMMB Bank and JMMB Cambio operations are the only permitted persons in the group, as such the other entities are therefore **not** allowed to transact business in cash over JA$1M, that is:

- Jamaica Money Market Brokers Limited
- JMMB Securities Ltd
- JMMB Fund Managers Ltd
- JMMB Money Transfer Ltd
- JMMB Insurance Brokers

9 CLIENT DUE DILIGENCE

9.1.1 Standard Client Due Diligence Requirements

CDD refers to basic information that should be collected from all potential clients before they are approved for acceptance. The objective of CDD is to understand the client's business and the types of transactions it will likely engage in and assist in the identification of unusual or suspicious activity. CDD also assists in risk rating the client and identifying clients that may pose increased risks (i.e., risk rated as medium or high) for money laundering who may require EDD and increased monitoring. In addition to the documents and information required for each client type, JMMB will adopt the following principles and guidelines for CDD:

9.1.1.1 Acquiring Knowledge and Understanding of the Client

1) JMMB should gain sufficient knowledge about its clients to ensure that it is doing business with reputable clients and suppliers whose association with JMMB will not expose the company to negative publicity.

2) Additional enquiries should be made to verify information if there appears to be doubt or inconsistency in the information provided.

3) Any update or change in existing information on the client that is in accordance with the KYC Policy should be documented and included on the client's file.

4) JMMB, at its discretion, may request additional information from clients in order to corroborate any information previously supplied by them

5) In accepting business from clients who reside overseas, JMMB will ensure that:
    1) Documents presented are certified/notarized
    2) Documentation presented is verified by contacting a third party

3) Original Certificates of Good Standing for corporations registered overseas are obtained

6) JMMB will not facilitate any wire transfers or other electronic fund transfer activities for persons who are not client of the institution.

7) Where funds are wired on behalf of professional intermediaries, all the relevant information must be obtained before such transaction is executed.

9.1.1.2 Verification and Review of Client Information by Team Members

The team member opening the account is required to examine the identification carefully to ensure that it is not forged or altered and that the description on the ID is consistent with the appearance of the person who presents it.

The particular type of account or services being applied for should not unduly influence the process of verification. It is important to obtain references from banks and other professional firms. These references should be requested by JMMB and be received directly from the banks and other firms providing such references. References and document confirmations must be verified. Reference is not required for a "long-standing client".

Each team member is required to check that all information in relation to the client is valid and is corroborated based on references and documents provided to support information included on the Client Information Form. All accounts designated as "High-Risk" must be referred to the Compliance Department.

It is acknowledged that there will sometimes be cases, particularly involving young persons and the elderly, where the appropriate documentary evidence of identity and

independent verification of address are not possible. All such cases are to be referred to Compliance for sign-off before the account is opened.

9.1.1.3 Review and Update of Existing Client Information

1) Each client-facing team member must undertake regular reviews (including retrospective reviews) of all existing client records (identification and other particulars) to ensure that they remain up-to-date, relevant, and consistent with JMMB's risk profile of that customer.

   These reviews shall be done on a continuous basis, but in any case, at least seven (7) years from the date of the commencement of the relationship and at minimum seven years increments thereafter, or, at more frequent intervals to ensure the accuracy of the information held by the institution or as warranted by the risk profile of the relationship.

2) At any time after the client relationship is established, the Compliance Department may request team members to contact the clients to obtain certain KYC information or documentation. Team members should contact the client to request the information and conduct any required follow-up considered necessary. Once the information and/or documentation is received, the team member should communicate with the Compliance Department where necessary and update the client record.

9.1.2 Enhanced Due Diligence Requirements

In addition to obtaining the required information and documentation to satisfy the requirements of CDD process, team members and the Compliance Department may also be required to conduct EDD on potential or existing clients that have been determined to be high risk, engaging in high-risk activities, business, foreign countries, linked accounts and PEPs.

Such accounts will require sign off from senior management for the establishment of the account.

EDD requirements may include the following:

1) Searches of databases and websites for additional information that may be available. This includes general searches on Google, local or international newspapers, and regulatory organisations' websites in other countries.
2) OFAC list
3) Screening Online Application
4) Independent confirmation with overseas or local entities and individuals
5) A report on the physical site visit that was conducted by the Relationship Managers to the Applicant's principal office and/or operating location. The report should contain the following information:
    a. the address visited;
    b. date of the visit;
    c. the name(s) of the person(s) visited and their positions within the organization or relationship to the company;
    d. a general description of the visit (e.g. business topics discussed);
6) Information regarding the AML supervisory and law enforcement regime of the jurisdiction that issued the licence to the company and of the parent entity if the institution is regulated, whether locally or overseas.
7) Information regarding whether the client has been subject to any criminal, civil or regulatory enforcement actions;
8) Other information that may be required based on the circumstances of each case.

9.1.3 Clients Requiring EDD

9.1.3.1 Politically Exposed Persons

Enhanced due diligence is required for transactions involving high-risk activities, businesses in foreign countries and PEPs.

PEPs are individuals who are or have been entrusted with prominent public functions including:

1. heads of state or government
2. senior politicians
3. a member of any House of Parliament
4. a Minister of Government
5. senior government Officers
6. a member of the judiciary
7. a military official above the rank of Captain
8. a member of the police force above the rank of Assistant Commissioner
9. a Permanent Secretary, Chief Technical Director or chief officer in charge of the operations of a Ministry, department of Government, executive agency or statutory body
10. A director or chief executive of any company in which the Government owns a controlling interest.
11. senior executives of publicly owned corporations
12. an official of any political party
13. an individual who holds or has held a senior management position in an international organization
14. an individual who is a relative or is known to be a close associate of a person described in point 13 & 14 above
15. immediate family. i.e. parent, sibling, spouse, children, in-laws as well as close

associates – that is – (persons known to maintain unusually close relationships with these persons)

The identity of the client must be ascertained and enhanced due diligence (see below) must be applied. This includes:-

1. Stricter KYC procedures – e.g. more detailed information on background, reputation etc.
2. Tagging of all such accounts in the system
3. Approval from Group Chief Compliance Officer, Country Compliance Officer or their designate, to open these accounts. Where the business arrangement has already commenced, approval will be required to continue the relationship.

9.1.3.2 Accounts opened by Professional Intermediaries

This group includes pension funds, unit trusts, and other fund managers, as well as lawyers, security dealers and stock brokers managing single or pooled accounts held on deposit or in escrow.

If JMMB determines that the account is being held on behalf of a single client, then the identity and the relevant KYC information for that client must be ascertained.

Where pooled accounts are maintained, JMMB may rely on the professional intermediary's due diligence process and not look through to the ultimate beneficiary, but only if the following conditions obtain:

1. The intermediary engages in sound due diligence practices;
2. JMMB is able to verify the reliability and effectiveness of the intermediary's client due diligence.

3. Valid Power of Attorney in effect
4. The intermediary is held to a high standard of best practice

9.1.3.3 One-Off Transactions and Introduced Business

One-Off Transactions

These are transactions which are done by clients who are not account holders. They include:

- Purchasing of Bonds / Debentures / Locally Registered Stock (LRS);
- Cambio transactions
- Bank Transactions
- Fund management transactions etc.

We **must** get the required KYC information outlined above from these clients for all such transactions. A client record must also be created in the system for these clients.

Introduced Business

In circumstances where business is being introduced by individuals or companies, JMMB has the ultimate responsibility to do its due diligence on the referred client. Reliance should not be placed solely on the introducers.

Non-Face-to-Face Clients

For prospective clients who wish to open accounts and execute transactions via email, website or post, higher standards of scrutiny and due care must be applied and the following should be noted:-

1. More rigorous identification and verification standards must be applied and this includes:
    a. Copies of documents presented are certified by the relevant and appropriate authority;

b. Customers must submit additional documents to verify identity, the intended nature of the business relationship, as well as the reason(s) for the intended or performed transaction/(s);
c. If possible, face-to-face contact must be made with the customer
d. The first payment must be made through a financial institution which has similar CDD standards. It may also be necessary for financial institutions to increase the number and timing of controls and checks applied during the course of the business relationship including selecting patterns of transactions that will be subject to further examination.
e. Requesting current bank statements

2. Until physical verification of the client is performed encashments or withdrawals from the account must also be made to the account holder. If to a third party, approval must be sought from the Branch Manager or designate.

Please note that all information must be validated before the account is opened. Copies of all documents must be signed and sealed by a Notary Public resident in the country of origin. Existence of notary public must be verified and verification filed with account-opening documents

10 NON-CO-OPERATIVE COUNTRIES AND COUNTRIES WITH INADEQUATE AML/CFT FRAMEWORKS

JMMB will periodically provide information on the list of Non-Co-operative Countries and Countries with inadequate AML/CFT frameworks that are categorised as a significant threat to the Counter-financing of Terrorism. The countries included in this list are subject to change and will be communicated by the Compliance Department from time to time. The current list of countries includes:

1) Countries subject to United Nations Sanctions.
2) Counties subject to prohibitions in the U.S. Office of Foreign Asset Control (OFAC).
3) Countries with poor records of combating money laundering and terrorist financing or which are the subject of considerable unrest and lack of political stability.

Clients with origins or links to countries on this list may not be accepted as clients of JMMB without the prior approval of the JMMB Compliance Manager.

Countries on the OFAC and UN Sanctions List and FATF-Monitored Jurisdictions:

Afghanistan	Lao People's Democratic Republic
Balkan	Lebanon
Bahamas	Libya
Belarus	Mongolia
Bosnia & Herzegovina	North Korea
Botswana	Panama
Burma (Myanmar)	Rwanda
Burundi	Pakistan

Cambodia	Russia
Cote d'lvoire	Sierra Leone
Crimea	Somalia
Cuba	Syria
Democratic People's Republic of Korea	Sudan
Democratic Republic of Congo	Tanzania
Ghana	Trinidad & Tobago
Iceland	Uganda and Zaire
Iran	Vanuatu
Iraq	Venezuela
Liberia	Yemen
	Zimbabwe

Non-Cooperative Countries under the FATF List	
1. Myanmar (Burma)	
2. Nigeria	

Particular care should be taken when establishing relationships with clients from jurisdictions known to have weak Anti-Money Laundering and Countering Financing of Terrorism Regulations or with entities where there is no regulatory oversight by an independent body.

11 ADDENDUM I - JMMB BANK (JAMAICA) LIMITED ("THE BANK", "JMMB BANK")

Whilst JMMB Bank (Jamaica) Limited is covered under the JMMB Group (Jamaica Entities) AML/CFT and KYC Policy Manual, this addendum serves to highlight some of the pertinent aspects of the JMMB Bank's AML/CFT programme.

11.1 JMMB BANK'S AML/CFT COMPLIANCE PROGRAMMEME

The Chief Compliance Officer (CCO) for JMMB Bank (Jamaica Limited ("the Bank", "JMMB Bank") is responsible for the Bank's internal Compliance Program meme including the establishment of an adequately resourced unit that is responsible for the day-to-day monitoring of compliance.

JMMB Bank is required to implement an effective AML/CFT Compliance programme to ensure compliance with all laws, regulations, and guidelines affecting the entity (both locally and overseas). The programme must include the following areas which are detailed further in this and other relevant sections of the policy or in the JMMB Bank AML/CFT Compliance Procedures:

- The documentation, verification and due diligence requirements for new and existing clients including whether any of the clients meet the [2]US Indicia under FATCA.
- The nature and frequency of account and transaction monitoring including procedures for analysis of client's transactions to ascertain trends and to recognize indicators of unusual and/or suspicious activity over time.
- The internal and external reporting framework for suspicious transactions.
- The frequency, nature and scope of AML/CFT compliance testing.

- The nature and scope of AML/ CFT training.

- The follow-up of exceptions to ensure that timely corrective actions are taken and reporting on compliance levels including exceptions to senior management.

- Compliance risk assessments for new products and services.

- The frequency of consultation with the Designated Authority to ensure that the Bank is carrying out its obligations under the law.

- Periodic reviews of the AML/CFT programme including the Compliance Unit by internal and external auditor functions.

- The provision for the heightened scrutiny of certain categories of clients and the types of transactions when necessary as well as the continuous review of existing practices and procedures in this area.

- The documentation of procedures for analysis of transactions (other than client-related transactions) that are undertaken in the course of business to determine whether the transaction is one in relation to which a required disclosure must be made. Such transactions could include the following:

    - Corresponding banking arrangements,

    - Proprietary transactions such as security transactions,

    - Fixed assets acquisitions and disposal, and

    - Custody arrangements

A comprehensive AML/CFT compliance plan should be developed and submitted to the Board of Directors for approval annually by the Bank's Chief Compliance Officer. The plan should outline the strategies to be put in place to improve the compliance programme for the Bank. The plan should provide for ongoing independent review and testing of team member compliance with AML and CFT requirements.

11.2 ROLES AND RESPONSIBILITIES

The following sections outline the roles and responsibilities of the Board of Directors, the Audit Committee of the Board, the Senior Management, Internal Audit Department, the Culture and Human Development Team, the Compliance Unit, the Chief Compliance Officer, Designated Compliance Officers, Relationship Managers/Officers and Team members who are critical to the AML/CFT Programme. The specific responsibilities for each grouping are as follows:

11.2.1 THE BOARD OF DIRECTORS

The ultimate responsibility for compliance with the AML/CFT Policy and Procedures lies with the Board of Directors.

The Board of Directors must have a clear understanding of the Money Laundering (ML) / Terrorist Financing (TF) risk faced by the Bank. This includes a good working knowledge of the operating risks faced based on the products offered; client base; strength of internal controls and hiring policies.

In order to fulfil its obligations, the responsibilities of the Board of Directors include:

- Approving the AML/CFT Policy and any amendments thereto.
- Appointing a Chief Compliance Officer/Nominated Officer, who is appropriately qualified and has the requisite stature and authority to undertake the responsibilities of that function and to effectively execute the function.
- Approving the compliance plan.
- Approving waivers from Threshold reporting for clients as may be recommended by the CCO from time to time.
- Requiring and reviewing compliance and audit reports which should address regulatory compliance as well as compliance with internal controls and corrective measures instituted (where necessary).

- Requiring that reports by the Nominated Officer are provided with a frequency that accords with the risk profile of the Bank.

- Requiring that the Bank has adequate policies and processes for screening prospective and existing team members to ensure high ethical standards.

- Ensuring that the Bank's risk assessment accurately and appropriately reflects the ML and TF risks inherent in the institution and that the risk assessment accurately reflects the effectiveness of the mitigating controls and is updated on an ongoing basis.

- Ensuring it receives adequate and appropriate exposure to training materials and updates on the local AML/CFT laws and framework as well as international standards of best or sound practices which impact AML/CFT obligations for financial institutions. Ensuring the Bank's AML/CFT policies and procedures are effectively implemented.

The effective implementation of the Bank's policies and procedures means:

- The frequency and content of AML/CFT training should be aligned with team members' roles and functions;

- The internal audit function assesses the risk management practices and internal controls of the Bank including periodically assessing the effectiveness of its compliance with its AML/CFT policies and procedures
-
- Compliance and oversight functions are provided with adequate or sufficient resources to ensure that AML/CFT policies and procedures are effectively implemented; and

- The external audit function engagement extends to the institution's compliance with its AML/CFT policies and procedures.

11.2.2 THE AUDIT COMMITTEE

The Board has delegated responsibility for overseeing the AML/CFT compliance function to the Audit Committee of the Board. The role of the Audit Committee in relation to AML/CFT Policy includes:

- Reviewing and recommending proposed amendments to the JMMB Bank's AML/CFT Policy Manual before they are submitted to the Board of Directors for approval.

- Reviewing internal and external audit reports on the AML/CFT Program meme and Plan.

- Reviewing reports prepared by the Bank's Chief Compliance Officer on the organization's compliance programme and Plan and making appropriate recommendations to the Board of Directors in respect thereof.

- Reviewing the results of AML/CFT examinations, compliance reviews, audits and independent testing, as well as corrective actions planned or taken in response thereto.

- Monitoring on-going AML/CFT activities and issues by receiving and reviewing reports provided by the Compliance Department.

11.2.3 SENIOR MANAGEMENT

For the purposes of this Policy, "Senior Management" is comprised of the officers of the Bank who form the leadership team with the responsibility of managing the bank. Senior Management is responsible for ensuring that:

- A strong culture of AML/CFT compliance is upheld among JMMB Bank's business and support units inclusive of subsidiaries (if any).

- Each business unit takes ownership and is held accountable for implementing the AML Policy by integrating applicable components of the Policy into its business operations (including KYC Policies) and takes corrective actions when breaches are identified.

- The Chief Compliance Officer has access to required information and personnel.

- Roles and responsibilities relating to the AML/CFT policies are communicated to JMMB Bank personnel;

- The programme is observed;

- The business units have adequate staffing to support the reasonable performance of the AML/CFT functions and responsibilities; and

- Appropriate remedial or disciplinary action is taken if breaches are identified.

11.2.4 INTERNAL AUDIT DEPARTMENT

Internal audit is responsible for coordinating and conducting independent reviews of the AML/CFT programme at least annually. Internal Audit will report the results of such independent reviews to the Audit Committee and any other committees or members of senior management as appropriate.

11.2.5 THE CULTURE & HUMAN DEVELOPMENT TEAM

The responsibility of the Culture & Human Development Team with respect to the AML/CFT programme include:

- Applying appropriate disciplinary action, including termination of employment, when team members fail to comply with AML/CFT laws or regulations or AML/CFT policies and procedures.
- Ensuring the CCO has the qualifications and experience needed for the position.
- Working with the business units to determine how best to incorporate compliance in performance evaluations and incentives.
- Implementing a comprehensive screening process involving the investigation of the background, integrity and competence of team members prior to employment and during employment as may be required.
- Assisting the Compliance Unit in the KYE Process to ensure that all team members maintain fit and proper status; this includes getting the relevant documents on the commencement of employment.
- Working with the Compliance Unit in ensuring that all team members receive the annual AML/CFT Training.
- Ensuring CCO and Designated Compliance officers receive annual training in their area as required by the regulations.

- Implementing policies and procedures with respect to KYE to ensure that employees are fit and proper persons. See Section 11 of this document, "Employee Integrity & Awareness" for details on the KYE requirements.

11.2.6 THE COMPLIANCE UNIT

Through the leadership of the Bank's Chief Compliance Officer (CCO), the Compliance Unit provides AML/CFT oversight and support to business and support units in establishing and implementing procedures for compliance with the applicable AML/CFT laws and regulations and regulatory guidelines. The primary responsibilities of the Compliance Unit include:

- Evaluating laws and regulations, with the guidance of internal and external counsel, to determine their applicability to JMMB Bank and subsidiaries (if applicable).
- Performing assessments across the operations to identify and evaluate compliance risks and controls for detecting breaches with the relevant laws, regulations and bank policies, including proposed new products or services or variations in existing products and services.
- Developing and implementing appropriate compliance training and employee awareness programmes.
- Providing guidance to business units on the applicability of laws, rules and regulations to new products.
- Reviewing clients requiring EDD, including those risk rated as high.
- Conducting routine and targeted compliance testing of the business units related to AML/CFT procedures.
- Identifying, monitoring, and investigating any potentially suspicious activity identified by monitoring systems and referred by business units as well as making the appropriate reports to the Designated Authority.
- Conducting investigation and verification of information for clients requiring EDD.
- Appointing Designated Compliance Officers.

11.2.7 THE BANK CHIEF COMPLIANCE OFFICER (CCO)

The CCO is responsible for overseeing and managing the AML/CFT plan and programme. The CCO will be the Nominated Officer for the Bank, in accordance with the

Proceeds of Crime Act and should be at senior management level to allow for reporting to the Board or through a committee of the Board. The Nominated Officer should be independent of the business lines of the Bank to allow for an objective assessment, monitoring and enforcement of the Bank's operations and decision making in accordance with its AML/CFT obligations under the country's framework and with the Bank's own AML/CFT policies and procedures. All references to the Nominated Officer in this document should be interpreted to mean the CCO.

The CCO is responsible for:

1. Being fully acquainted with the provisions of the Proceeds of Crime Act, the Terrorism Prevention Act and their amendments from time to time and their supporting regulations in addition to all other laws and guidelines affecting the entity. She/he must, in particular, be cognizant of the confidentiality requirements with regard to reporting transactions.
2. Remaining informed of the local and international developments on money laundering and terrorist financing and industry best practices that can guide the Bank in establishing and maintaining the requisite controls, policies and procedures in accordance with statutory requirements and related the framework
3. The training of all team members of JMMB Bank with respect to the AML & CFT programme and the applicable regulatory and legal requirements.
4. Ensuring that all team members are kept up to date on current legislative requirements, both international and local.
5. Establishing a compliance plan which will include on-going and independent review and testing of staff compliance in order to achieve the KYE requirements.
6. Implementing programmes, policies, procedures and controls to detect money laundering and terrorist financing activities.
7. Establishing a reporting system whereby team members can report activities which are not in compliance with the Bank's policies without fear of retribution.
8. Submitting monthly and annual reports on the compliance programme to the Board of Directors and Senior Management.
9. Having regular consultation with the Designated Authority and the Competent Authority to ensure that the Bank is carrying out its obligations under the laws.
10. Ensuring all such activities as required by the relevant statutes and Guidance including but not limited to Threshold Transactions, Suspicious Transactions and Listed Entities are submitted to the FID in a timely manner.
11. Ensure that the applicable reporting under FATCA is submitted in a timely manner.
12. Ensure that all submissions due to the JDIC are submitted within the requisite time and that the Bank is in compliance with the JDIC record-keeping guidelines once fully implemented.

13. Providing guidance and advice to team members on the identification of Suspicious Transactions and evaluating reports of Suspicious or Unusual Transactions and verifying whether they are subject to reporting.
14. Providing on-going training to the Compliance Officers.
15. Acting as liaison between the Bank and regulatory and law enforcement agencies with respect to all compliance matters and investigations.
16. Monitoring and ensuring that all exceptions are addressed.
17. Ensuring that adequate resources are in place to effectively monitor compliance.
18. Evaluating new products and services to determine the level of risk and making appropriate recommendations.
19. Liaising with the Bank's legal and audit departments on AML/CFT matters and investigations.
20. Identifying training programmes for Compliance Officers and Bank team members that will mitigate the risk of non-compliance or breaches of the various regulations.
21. Making recommendations with respect to the Code of Conduct and Ethics disseminated to team members.
22. Implementing recommendations from Internal Audit.

11.2.8 DESIGNATED COMPLIANCE OFFICERS

The Designated Compliance Officers at the branches support the Compliance Unit by obtaining, reviewing and confirming the completeness of KYC information and the quality of the documentation gathered during the client acceptance process and throughout the duration of the relationship with the client. The responsibilities of the Designated Compliance Officers with regards to KYC also include:

- Reviewing and signing-off on the completed KYC file, including approval of any change in the client static data.
- Forwarding KYC-related documents to the Compliance Unit for further analysis when appropriate.
- Ensure that each client is assigned a Relationship Manager (RM).
- Conducting initial client due diligence checks (i.e., OFAC, UN Sanction listing, [3]"PEPs, and adverse searches), maintaining evidence of such checks, and escalating any issues to the Compliance Unit.

[3] Individuals (both local and foreign) entrusted with prominent public functions, their families and close associates.

- Maintaining vigilance in the normal course of duties to identify and escalate unusual or suspicious activity.
- Submitting, upon request, periodic reports to the Chief Compliance Officer on the following:

    i. new accounts opened in a given period;
    ii. existing accounts for which additional KYC information is outstanding;
    iii. accounts reactivated from dormancy or closed in a given period.

11.2.9 RELATIONSHIP MANAGERS/OFFICERS (RM/RO)

RM have primary responsibility for the relationship with the client and are ultimately responsible for forming a reasonable belief of the true identity, place of birth, nationality(ies), permanent residence and residency status of a client and can reasonably establish expected and usual activity. An RM or RO is assigned to each client relationship and this assignment remains for the duration of the client relationship until the resignation of the RM or amended by the Business Unit Heads.

The RM's or RO's responsibilities with regards to KYC are as follows:

- Interacting with a client to obtain all required KYC information and documentation prior to account opening as well as interacting with a client to update any KYC information or documentation as part of on-going reviews/updates.
- Interacting with the client to ascertain whether the client meets the US Indicia in keeping with FATCA.
- Interacting with the client to ensure the client understands the client information verification requirements and other KYC requirements.
- Forming a reasonable belief on the true identity of each client based on the requisite due diligence and communicating this by signing-off on the completed client information file to confirm the accuracy and completeness of the client file.
- Serving as a point of contact and providing business subject matter expertise to assist in resolving unusual or suspicious activity investigations. The RM or RO also escalates potentially suspicious activity through the appropriate channels.
- Maintaining vigilance in the normal course of business to identify and escalate unusual or suspicious activity as required by JMMB Bank's suspicious activity escalation procedures.
- Participating in updating clients' KYC files and periodically confirming that a client's information and risk rating is accurate and up-to-date.

- Participating in targeted KYC and AML/CFT training.

For the purposes of FATCA compliance the RM is required to know his/her clients to the extent that he/she should be able to:

- indicate any accounts that are directly or indirectly owned by the same person, as well as all accounts the RM has associated with one or another through a relationship code, client identification number, tax identification, or similar indicator; and
- In the case of accounts with a balance of more than US$1,000,000 (after aggregation in keeping with the above), advise whether the account holder is a U.S. citizen or resident.

11.2.10 ALL TEAM MEMBERS

Team members should be aware of and comply with requirements regarding the AML/CFT programme, the JMMB Group Code of Conduct and Ethics and the internal policies, procedures and processes of the Bank. Any employee that suspects or learns that a transaction or account is unusual, or that transactions are being structured to evade any anti-money laundering or FATCA requirements must promptly notify his/her supervisor or the Compliance Unit. The CCO will take steps to investigate, limit, close or otherwise restrict the account and bring the matter to the attention of Senior Management and the appropriate Committee of the Board and consider whether an STR should be filed.

12 COMPLIANCE MONITORING AND TESTING

12.1 EMPLOYEE MONITORING OF TRANSACTIONS AND ACCOUNT ACTIVITY

1) Team members who manage the client relationship or accept and process client transactions are the first line of defence in understanding the normal and expected activity of a client and are therefore in the best position to monitor transactions.

2) All RMs must be vigilant in identifying changes in client transactions that appear inconsistent with the expected transaction type and activity level for the client. Where such change in activity level is identified, the RMs must communicate with the client and obtain up-to-date information including any expected change in profile or activity levels. Such information should be documented via file notes and inserted on the client static files. If the RM believes the particular transaction or trend is unusual based on the understanding of the client, such transaction should be reported immediately to a Compliance Officer or the Compliance Unit.

3) Compliance Officers must also be vigilant in identifying changes in the transaction or activity trends of particular clients and seek additional information from RMs or communicate directly with the Compliance Unit.

4) Where outstanding information is identified in relation to particular clients, these should be requested from the designated RM where applicable.

12.2 COMPLIANCE UNIT MONITORING REVIEW AND TESTING

In relation to the monitoring of transactions, the Compliance Unit is responsible for the following:

1) Daily monitoring of transactions and, where necessary, performing historical analysis of client accounts or transactions.

2) Ensuring the names of new and existing clients are automatically compared to the most recent OFAC List and UN Sanction list. A report is generated on a weekly basis which must be

reviewed to determine whether further investigations are required for any client names identified or whether a STR should be filed.

3) Reviewing of client accounts classified as high-risk accounts.

4) Reviewing high-risk accounts before the relationship is established.

5) Working closely with the regulators and keeping abreast of international media in identifying changes to the persons associated with illegal activity, non-cooperative countries, countries with weak AML/CFT frameworks and individuals and organizations associated with terrorism.

6) Adopting a consolidated approach in the assessment of clients with multiple accounts within the Bank. These will be reviewed periodically by the Compliance Unit.

12.3 INDEPENDENT AUDIT OF COMPLIANCE PROGRAMME

The internal auditor will conduct a review of the AML/CFT Compliance framework to determine the effectiveness of the compliance programme in place. This review will incorporate at a minimum:

1) An assessment of:
   - the duties and responsibilities of the Compliance Officers
   - the adequacy of the AML/CFT policies and procedures
   - the AML/CFT training programme
   - the integrity and reliability of the systems used for AML/CFT compliance

2) The selection of accounts, on a sample basis, to ensure adherence to policies and procedures and the regulations and guidance notes issued by the regulators.

The findings and recommendations of the audit should be communicated to the Compliance Department, Senior Management and Audit Committee as well as any other relevant individuals or departments.

The Internal Audit Department may also coordinate with the Compliance Unit, as it deems necessary or appropriate in order to resolve matters arising in connection with the Bank's AML, CFT and KYC policies and procedures.

JMMB Bank may request an independent audit of the AML Compliance Programme to be conducted by the external auditors to assess its effectiveness. The Internal Audit Department and the Audit Committee should be consulted where appropriate.

12.4 ANNUAL REPORT TO THE BOARD OF DIRECTORS

The Chief Compliance Officer must submit an Annual Compliance Report to the Board of Directors within four months of the end of the financial year. The report should include the following:

a. An Overview and evaluation of the overall effectiveness of the AML/CFT Framework

b. The effectiveness of the AML/CFT measures implemented in the various operational areas and for applicable products and services.

c. The AML/CFT training exercises completed during the year and the results of the initiatives pursued for the year.

d. All major issues identified in relation to the AML/CFT Compliance Programme and how these were addressed during the year.

e. The Bank's compliance with relevant legislation and the BOJ Guidance Notes.

f. The number and frequency of threshold and suspicious transactions detected and reported as well as matches and Listed Entities reports made to the Designated Authority.

g. The number of clients reported under FATCA.

h. Any significant and/or unusual trends arising from a review of transactions detected and reported as it relates to specific branches, geographic areas or types of transactions.

i. The level of compliance in relation to client due diligence standards.

j. The level of compliance in relation to updating of existing client records.

k. Reporting on the findings of the AML/CFT audits undertaken by the internal or external auditors and the responses and remedial actions to findings from the Regulator's examination.

l. Assessment as to the effectiveness of monitoring high-risk clients and information on any challenges identified during the year with respect to these client types.

m. Update on programmes employed during the year to ensure employee awareness and integrity including the effectiveness of the training programmes.

n. Update on the Bank's relationship with the Designated Authority and the overall guidance received.

o. Advice on the impact of any proposed or impending legislative or regulatory changes on the AML/CFT programme and recommendations to ensure continuing compliance.

p. Report on all relationships terminated during the period due to issues in relation to AML/CFT compliance.

APPENDIX I – EXAMPLES OF ACTIVITIES THAT MAY GIVE RISE TO SUSPICION

This appendix provides team members with examples of unusual activity, regardless of whether a specific transaction type is involved. This list is not exhaustive, but is provided to assist team members in understanding transactions which could be unusual when compared to a client's expected pattern of activity.

Red Flags related to Client Behaviour

During the Client On-boarding or Account-Opening Process

- The client wishes to engage in transactions that lack business sense, apparent investment strategy, or are inconsistent with the client's stated business or strategy.
- The client exhibits unusual concern for secrecy, particularly with respect to his identity, type of business, assets or dealings with firms.
- The client displays reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the financial institution to verify.
- The client refuses to identify or fails to indicate a legitimate source for his funds and other assets.
- The client is unconcerned with risks, commissions, or other transaction costs.
- The client appears to operate as an agent for an undisclosed principal, but is reluctant to provide information regarding that principal.
- The client has difficulty describing the nature of his business and lacks general knowledge of his industry.
- For no apparent reason, the client has multiple accounts under a single name or multiple names.
- The client is from, or has accounts in, a country identified as a haven for money laundering.
- The client does not wish to receive faxes or mail nor to correspond with you in writing or have any direct contact with you.
- The client, or a person publicly associated with the client, has a questionable background, including prior criminal convictions.
- Use of a mailing address, particularly a P.O. Box, only.
- Unwillingness to disclose identity of ultimate beneficial owners.

On-Going Monitoring of Client Account

Client account monitoring must be intensified with regard to:

- A refusal by a client to provide complete evidence of identity.
- The client trying to carry out all his business orally as opposed to in writing.
- The clients' account having inflows of funds or other assets well beyond the known income or resources of the client.
- The client operating a local business and using foreign currencies for the vast majority of business transactions.
- The client activating his accounts suddenly which are then being used in an unusual manner, especially for transferring large amounts from other countries.
- The client keeping a number of accounts where the nature of his activity does not require this, especially if transactions on these accounts take place with individuals of no clear relationship with the client.
- The client depositing and withdrawing large cash amounts not matching the nature of his activity.
- The client having huge amounts of cash passing through his account and not using other banking instruments, for no clear reason.
- The frequent requests for converting cash deposits to other payment means with amounts not matching the client's activity.
- The client utilizing several accounts for depositing large amounts of cash within a short period of time.
- The sending or receiving transfers in huge amounts without clear reason and they are not in line with the nature and volume of his activities, especially with instructions to make cash payments.
- Transfers received regularly, and in large amounts, from countries involved in drugs trafficking or supply, which have a strict system for the secrecy of bank accounts or have no or inadequate legislation for combating money laundering.
- The client whose high account turnover is inconsistent with the size of the balance (suggesting that the funds are being "washed" through the account).
- The client with a dormant account who suddenly receives a deposit or series of deposits followed by daily cash withdrawals that continue until the transferred sum has been removed.

Red Flags Related to Excessive Secrecy

- Excessive or unnecessary use of nominees.
- Unnecessary granting of power of attorney.
- Using a client's account rather than paying for things directly.

Red Flags Related to the Client's Behaviour

- The purchase of companies which have no obvious commercial purpose.
- Sales invoices totals exceeding known value of goods.
- The client who sells at an undervaluation.
- The client who makes unusually large cash payments in relation to business.

Red Flags Related to Corporate Structures

- Subsidiaries which have no apparent purpose.
- Companies which continuously make substantial losses.
- Complex group structures without a cause.
- Uneconomic group structures for tax purposes.
- Frequent changes in shareholders and directors.

Red Flags Related to Introducers

- Introducer's creation of corporate vehicles or other complex legal arrangements serving to confuse the links between the proceeds of a crime and the perpetrator.
- Introducer fronting for criminals with a large amount of money to invest, posing as individuals hoping to minimise their tax liabilities or desiring to place assets out of reach, in order to avoid future liabilities.
- Agent, attorney or financial advisor acting for another person without proper documentation, such as a power of attorney.

Red Flags Related to Public Officials

- The client, who is a public official, opens accounts in the name of a family member who begins making large deposits not consistent with the known legitimate sources of income of the family.
- The client, who is related to a public official, makes large deposits not consistent with the

client's own legitimate sources of income.

Red Flags Involving Financial Institution Team Members and Agents

- Changes in team member characteristics, e.g., lavish life-styles or avoiding taking holidays.
- Changes in team member's or agent's performance, e.g. the salesman selling products for cash has remarkable or unexpected increase in performances.

Red Flags Related to Cash Transactions

- Unusually large cash deposits or payments made by an individual or company whose business activities would normally be generated by cheques, banker's drafts or other instruments.
- Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period, out of the account and/or to a destination not normally associated with that client.
- The client who deposits cash by means of numerous different deposits so that the total of each deposit is insignificant, but the total of all the credits is significant.
- Clients who constantly pay in or deposit cash to cover requests for banker's drafts, money transfers or other negotiable and readily marketable money instruments.
- Clients who seek to exchange large quantities of low denomination notes for those of higher denomination.
- Frequent exchange of cash into other currencies.
- Clients who numerous cash transactions than usual.
- The client transferring large sums of money to or from overseas locations with instructions for payment in cash.
- Requests to open an account with a substantial deposit of cash or other bearer instrument to facilitate the payment of insurance premium or to fund a trust.

Red Flags Related to Bank or Trust Accounts

- The client who wishes to maintain a number of trustee or client accounts, which do not appear consistent with the type of business, including transactions which involve nominee names.
- Request to form or act as Trustees for Trusts where it is difficult to identify the rationale behind the Trust or the source of funds to be held in the account and the identities of the

beneficiaries.

- Matching of payments out with credits paid in by cash on the same or previous day.
- Large cash withdrawals from a previously dormant/inactive account, or from an account which had just received an unexpectedly large credit from abroad.
- The client who uses separate tellers to conduct large cash transactions or foreign exchange transactions.
- Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other clients, company or trust accounts.
- Large numbers of individuals making payments into the same account without an adequate explanation.
- Unexplained transfers of significant sums through several bank accounts.
- Use of bank accounts in several currencies without reason.

<u>Red Flags Related to Secured and Unsecured Lending</u>

- The client who repays problem loans unexpectedly.
- Request by a client for a financial institution to provide or arrange finances where the source of the client's financial contribution to a deal is unclear, particularly where property is involved.
- Requests for loans to offshore companies, or loans secured by obligations of offshore financial institution.

APPENDIX II: EXAMPLES OF ACTIVITIES OR TRANSACTIONS THAT MAY GIVE RISE TO SUSPICION

- **INDIVIDUAL ACCOUNTS**

1. Client resides in country or region where high incidents of money laundering and terrorist financing are detected
2. Client introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent
3. Client unwilling to provide background information when being on-boarded
4. Client who tries to establish a relationship without references or refuses to provide other required on-boarding information
5. Client who presents unusual or suspicious documents that cannot be readily verified
6. Client who has no record of past or present employment but does large transactions
7. Client who tries to open account with large amounts of cash
8. Client who provides a residential contact number that is disconnected when called
9. Self-employed individuals who show large earnings that are not easily explained
10. Client whose net-worth increases exponentially within a short period of time and cannot account for this recent increase in wealth
11. Request for unexplained payment to third parties

- **CORPORATE ACCOUNTS**

1. Business that is reluctant to provide full information regarding purpose of business, prior banking relationships, directors or its location
2. Business that refuses to provide information for credit references
3. Business that is reluctant to reveal details about its activities or provide financial information when requested
4. Business introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking is prevalent
5. Business is reluctant or unable to furnish information on its principals and signing officers

6. Business not generating sufficient income, but consistently makes large cash deposits
7. Business builds up large cash balance, not consistent with the known turnover and subsequent transfer to account held overseas
8. Request for payment of an investment to a third party on maturity without valid reason

- **BORROWING RELATIONSHIP**
    1. Client who suddenly pays down a problem loan with no reasonable explanation of source of funds
    2. A request for loans to an offshore company, especially one that is located in a bank secrecy haven secured by obligations of an offshore bank
    3. A loan collaterized by an investment vehicle or cash deposit
    4. Where the proposed loan purpose does not make sense or the client is willing to provide cash deposit as collateral while refusing to disclose the loan purpose
    5. Client request to borrow against assets held by a third party, where the origin of the asset is not known or the asset is inconsistent with the clients' financial standing

- **CASH DEPOSITS OR INVESTMENTS**
    1. Business accounts whose deposits and withdrawals are primarily cash
    2. Client who operates a retail business and provides cheque cashing services but does not have large draws of cash against cheques deposited. This indicates another source of cash
    3. Unusual cash purchases to facilitate wire transfers
    4. Unusual volume of deposits in managers' cheques, money orders and travellers cheques, when the nature of the business does not justify such activity
    5. Accounts that show frequent large deposits and withdrawals to purchase managers cheques and other negotiable and readily marketable money instruments without a valid business reason
    6. A single substantial cash deposit composed of many small notes

7. Frequent exchange of cash into other currencies
8. Frequent exchange of small bills for large bills and vice versa
9. Sudden and inconsistent change in currency transactions or patterns
10. A depositor who purchases wire transfer with large amount of cash or just under a specified threshold without apparent reason (structuring)
11. A client who is reluctant to provide requested information
12. Client who opens a number of accounts under one or more names and makes deposits of less than US$15,000, or the equivalent in any other currency, in cash in each of the accounts
13. A client who makes deposits or investments of money orders carrying unusual symbols or stamps (these can be used as accounting tools by the drug cartel)
14. A client whose deposit or investment consistently contains counterfeit notes or forged instruments
15. A substantial increase in cash deposits or investments made by a client that is immediately transferred to a third part account or to a destination not normally associated with the client

- **INVESTMENT RELATED TRANSACTIONS**

1. A client consistently purchasing securities to be held in safe keeping by JMMB, where this does not appears to be appropriate given the clients financial standing
2. Settlement of securities by using large volumes of cash
3. Request by client for investment and portfolio management services in foreign currency securities where the source of funds is unclear or cannot be ascertained, and is not consistent with the client's financial standing
4. Low-graded securities purchased in an overseas jurisdiction are sold locally and the proceeds used to purchase high-graded security

- **WIRE TRANSFER ACTIVITY**

1. An account that sends and receives wire transfers, especially from bank secrecy haven countries or through countries that are known source of narcotics that is inconsistent with the client's business

2. An account that sends many small incoming wire transfers and immediately transfers the funds to another country
3. The deposit of funds into several accounts below the US$15,000, or the equivalent in any other currency, reporting threshold and then consolidating them into a master account and transferring them outside the country
4. Instructions received to wire transfer funds outside the country and to expect an equal incoming wire transfer from other sources
5. Receiving wire transfers and immediately purchasing managers' cheques for payment to a third party without a reasonable explanation
6. Clients who experienced increased wire transfer activity when previously there was no or irregular activities
7. International wire transfers for accounts with no history of such transfers or where the stated business does not warrant such activity

- **LETTERS OF CREDIT**

1. Unit pricing of items being financed seems unreasonable high
2. Movement of goods being financed is not consistent with the location of the parties to the Letter of Credit
3. Documents presented cannot be verified
4. Presentation of title documents with discrepancies waived
5. No proof of shipment required in documentation

- **EMPLOYEE ACTIVITY**

1. employee team member whose life style cannot be supported by his or her salary
2. employee team member who is reluctant to take a vacation
3. A team member who is associated with mysterious disappearances or unexplained shortages of the company's assets

- **REMITTANCE**

1. Customers who provide insufficient or suspicious information

2. Efforts to avoid reporting or recordkeeping requirements
3. Funds transfers to or from high-risk countries s
4. Activity inconsistent with customer's business
5. Unusual characteristics or activities
6. Unusual patterns of transactions
7. High volume of funds transferred compared to the socioeconomic profile of the client
8. Frequent transactions to different beneficiaries
9. Frequent transactions from multiple senders
10. Transfers to high-risk countries
11. Customer unwilling to provide information on transaction
12. Transaction amount just below the threshold
13. Small amounts sent frequently

- **INSURANCE BROKERAGE**

1. Premium inconsistent with client profile e.g. client purchases policies in amounts considered beyond apparent means
2. Large single premium deposits
3. Early termination of a policy at a high penalty after paying in cash
4. Client lacks concern for cost and performance of a policy but places greater concern in the early cancellation provisions of the policy
5. Client purchases a large insurance policy and within a short time period cancels the policy and requests that the cash value be paid out to a third party
6. Use of a third party cheque to purchase a policy
7. Overpayment of premium in order to get a refund
8. Client cancels policy and request return of premium in a currency different from the initial transaction currency
9. Client wants to borrow the maximum cash value of a single premium policy soon after making payment
10. Transfer of benefit of a policy to an unrelated third party
11. Client requests to make a large lump sum cash payment or pay with foreign currency

12. Policyholder makes frequent investments to a policy or number of policies and almost immediately withdraws most of the funds, leaving a small amount

APPENDIX III - LEGAL & REGULATORY FRAMEWORK

LOCAL LEGISLATION

The Proceeds of Crime Act, 2007 (POCA)

This Act is meant to represent an 'all crimes' approach to dealing with money laundering and generally the proceeds of crime. As such, it can now be seen that money laundering is any activity amounting to dealings with criminal property. Criminal property is any property that constitutes a benefit derived wholly or partially from criminal conduct. Criminal conduct means any conduct constituting an offence in Jamaica or if outside, conduct that would constitute a crime in Jamaica.

The responsibility for enforcing the provisions of the POCA is shared amongst the Asset Recovery Agency (ARA); the Director of Public Prosecutions (DPP); the Police, Customs, the Competent Authority (meaning any regulator authorised by the Minister), and any other person designated by the Minister.

Summary of the Proceeds of Crimes Act (POCA)

Under the Proceeds of Crime Act 2007 involvement in money laundering is an offence in Jamaica. POCA comprises seven parts which are summarised in the Bank of Jamaica guidance notes on the Detection and Prevention of Money Laundering and Terrorist Financing Activities (BOJ Guidance Notes) as follows:

- **Part I:** Provides provisions for the Assets Recovery Agency. Assets Recovery Agency under Section 3 means the Financial Investigation Division of the Ministry of Finance and Planning or any other entity so designated by the Ministry by Order.

- **Parts II, III, IV:** Deals with enforcement and investigatory tools such as Forfeiture Orders, Pecuniary Penalty Orders and Restraint Orders, Disclosure Orders, Search and Seizure warrants, Client Information Warrants and Account Monitoring Orders and the criminal lifestyle regime.
    - Under the POCA a person shall be deemed as having a criminal lifestyle if:

a. the person is convicted for an offence specified in the Second Schedule of the POCA;
b. the offence for which he is convicted or committed (by a RM Court whilst in custody or on bail) constitutes conduct forming part of a course of criminal activity, from which the person obtains a benefit; or
c. the offence for which he is convicted or committed (by a RM Court whilst in custody or on bail) over a period of at least one month and the person has benefited from the conduct constituting the offence.

- **Part V**: Deals with the issue of money laundering, required disclosures (STRs), and offences under the POCA. Under POCA money laundering is any act which:-
  - Constitutes an offence under Sections 92 (Concealing, etc. Criminal Property) or 93 (Acquisition Use, and Possession of Criminal Property);
  - Amounts to an attempt, conspiracy or incitement to commit an offence at Section 92 or 93 of POCA;
  - Amounts to aiding, abetting, counselling, or procuring the commission of an offence under section 92 or 93.

- **Part VI**: This part of the Act also deals with offences under the POCA. The offences addressed under this aspect of the Act are in relation to investigations being conducted.

- **Part VII**: Deals with matters general in nature such as regulation making powers under the Act, the repeal of the Money Laundering and Drug Offences and Forfeiture of Proceeds Act.

The POCA Money Laundering Prevention Regulations, 2007 (MLP)

The regulations outline the operational and regulatory control requirements that are to be implemented to ensure compliance with the POCA. The regulations detail the minimum documentation and operational procedures that should be maintained by financial institutions before commencement of a new business relationship or a one-off transaction.

Offences under POCA

Section 92 of the POCA creates an offence where a person:

- engages in a transaction that involves criminal property; or
- conceals, disguises, disposes of, brings into Jamaica, any such property; or
- converts or transfers or removes any such property from Jamaica

If that person knows or has reasonable grounds to believe at the time he does any act referred to above, that the property is criminal property (property that constitutes a person's benefit whether in whole, partially, directly or indirectly from criminal conduct).

Section 92(2) of the POCA creates an offence where a person enters into or becomes involved in an arrangement that facilitates the acquisition, retention, use or control of criminal property by or on behalf of another.

- For e.g. the issue of letters of credit on behalf of persons who proceed to use these arrangements to acquire property constituting criminal property also poses significant risks to financial institutions which can be liable under section 92(2) of POCA.

- Section 92(2) offence may also apply to cheque cashing, arrangements facilitating the movement of funds to accounts held (i.e. gift certificate arrangements) and currency exchanges.

See summary of major offences and the related fines in *Policy No. 25: Summary of Penalties for Non Compliances* of this policy document.

The Terrorist Prevention Act, 2005

Terrorist financing offences include:

a) Directly or indirectly, wilfully and without lawful justification or excuse collecting property, providing or inviting a person to provide, or make available property or other related services

- intending that they be used, or knowing that they will be used in whole or in part for the purpose of facilitating or carrying out terrorist activity and/or for the benefit of any entity known to be committing or facilitating any terrorist activity;
- knowing, that in whole or in part, they will be used by or will benefit a terrorist group

b) Facilitating or carrying out a terrorist activity by:
- using property directly or indirectly, in whole or in part; or
- possessing property intending that it be so used or knowing that it will be so used directly or indirectly in whole or in part

c) Dealing directly or indirectly in or with any property that is owned or controlled by or on behalf of a terrorist group

d) Entering into or facilitating, directly or indirectly, any transaction in respect of property owned or controlled by or on behalf of a terrorist group

e) Providing any financial or other related services in respect of that property for the benefit of or at the direction of a terrorist group;

(f) Converting any such property or taking any steps to conceal or disguise the fact that the property is owned or controlled by or on behalf of a terrorist group

Listed Entity

Financial Institutions must determine on a continuous basis whether they are in possession or control of property owned or controlled by or on behalf of a listed entity.

A listed entity is one that is included on a list of entities designated as terrorist entities by the United Nations Security Council and which the Designated Authority (The Chief Technical Director of the FID) has reasonable grounds to believe has knowingly committed or participated in the commission of a terrorism offence; or is knowingly acting on behalf of, at the direction of or in association with such an entity.

Fraudulent Transactions (Special Provisions) Act 2013

This new Act, enacted March 28, 2013, makes provisions for offences relating to fraudulent transactions and connected matters. New offences have been created including:

a. Stealing, forging or falsifying an access drive (the definition of access drive) would include an ETM card and a client's Moneyline PIN;
b. Possessing an instrument for use in either copying data from an access drive or forging or falsifying an access drive; and
c. Obtaining or possessing identifying information in circumstances which give rise to a reasonable inference that the information has been, or is intended to be, used to commit an offence.

The Act also requires that the Court orders a convicted person to give reimbursement (including interest accrued) to the victim of the offence. The impact of this legislation is that actions that may affect JMMB or its clients have been criminalized and JMMB or its clients may be able to get compensation for any loss suffered through those actions.

Local Regulatory Guidelines

Guidelines issued by Bank of Jamaica (BOJ)

Guidelines issued by the BOJ on "The Detection and Prevention of Money Laundering and Terrorist Financing Activities". This is applicable to Commercial Banks, Merchant Banks, Building Societies, Credit Unions, Cambios, Bureau de Change, Money Transfer and Remittance Agents and Agencies.

Guidelines issued by Financial Services Commission (FSC)

Guidelines issued by the FSC on "Anti-Money Laundering & Counter-Financing of Terrorism". This is applicable to entities regulated under the Insurance, Unit Trust, Pensions and Securities Acts and Regulations.

INTERNATIONAL REGULATORY FRAMEWORK

JMMB operates within the global financial industry and maintains correspondent banking and investment relationships with financial institutions operating outside of Jamaica. As a result, international regulatory requirements are important to achieve compliance required through correspondent relationships.

The major regulatory guidelines in relation to AML and the counter financing of terrorism governing the international financial community are as follows:

Basel Committee on Banking Supervision, 2001 – Client Due Diligence (CDD)
Discusses the Know Your Client (KYC) Framework which is to be used as a benchmark by financial institutions and banking supervisors to design and establish policies and procedures.

The USA Patriot Act, October 2001

- This legislation has expanded the Money Laundering laws of the United States and has placed more stringent procedural requirements on financial institutions. The United States Treasury now regulates the activities of the US financial institutions and in particular their relationships with foreign individuals and entities. The BOJ Guidance Notes highlights the far-reaching implications of this Act.

- This Act is considered significant due to its general power to cripple the financial services sector of any country. The Act allows US authorities to seize correspondent accounts held in US financial institutions for foreign banks which are in turn holding forfeitable assets. In addition, it grants the US Treasury and the US Attorney General power to issue a subpoena for summons to any foreign financial institution with a correspondent account within the United States requesting records relating to that account. The US Treasury or the US Attorney General may also direct a US Financial Institution to terminate the relationship with a foreign correspondent financial institution, if this financial institution fails to comply with a subpoena or summons.

The Foreign Narcotics Designation Kingpin Act and Regulations (The USA Drug Kingpin Act)

This Act was designed to deny significant foreign narcotics traffickers, their related businesses, and their operatives, access to the U.S. financial systems and all trade and transactions involving U.S. companies and individuals. The act authorizes the president to

take these actions when he determines that a foreign narcotics trafficker presents a threat to the national security, foreign policy, or economy of the United States.

USA Economic Sanctions Programme

The Office of Foreign Assets Control of the U.S. Department of the Treasury (OFAC) from time to time administers and enforces comprehensive sanctions programmes involving certain countries. As at March 2004, Cuba, Iran, Libya and Sudan were sanctioned countries. Therefore, unless authorised by OFAC, no U.S. person or company can do business with individuals, companies or government institutions in those countries or persons or entities acting for or on behalf of those countries.

The Financial Action Task Force on Money Laundering

The Forty+ Nine recommendations – June 2003 – This sets minimum standards for Financial Institutions to implement preventative measures to combat Money Laundering in accordance with legal and constitutional framework.

Guidance for Financial Institutions in Detecting Terrorist Financing – This describes the general characteristics of terrorist financing, which will assist financial institutions to be better able to protect themselves from being used as a conduit for such activity.

The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988 (Vienna Convention)

Jamaica being a signatory enacted the Money Laundering Act 1996 (and its amendments in 1997 and 1999) primarily in response to this convention.

The United Nations International Convention for the Suppression of the Financing of Terrorism 1999

Jamaica became a signatory on November 10, 2000. On September 16, 2005 Jamaica deposited with the U.N., instruments of accession to /ratification of this Convention

UN Resolution 1373(2001) on Threats to International Peace and Security caused by Terrorist Act

This Act mandates all member states of the United Nations to take action against individuals, groups, organization and their assets**.**

The Minister of Foreign Affairs and Foreign Trade receives from time to time an updated listing of individuals and entities which the United Nations has added to the consolidated list pertaining to Al-Qaida and other Terrorist Organisations. Local financial Institutions are required not to do transactions with these persons or entities, and report to Bank of Jamaica any existing transaction conducted with any name appearing on this list.

Foreign Account Tax Compliance Act (FATCA)

FATCA was enacted as part of the Hiring Incentives to Restore Employment (HIRE) Act of 2010. It requires financial institutions to use enhanced due diligence procedures to identify US persons who have invested in either non-US financial accounts or non-US entities in order to ensure that such persons are not hiding income and assets overseas. The primary goals of FATCA are to identify unreported income of US persons and to enlist the assistance of non-US financial institutions to report on such US persons.

APPENDIX IV - SUMMARY OF PENALTIES FOR NON-COMPLIANCE

Failure to comply with the regulations and guidelines in relation to Anti-Money Laundering and the Counter Financing of Terrorism may result in:

12.4.1 For JMMB:

1) Criminal Prosecution
2) Commercial Losses
3) Payment of significant fines
4) Legal and Reputational Risks
5) Negative Publicity
6) Suspension of license
7) Direct loss of revenue

12.4.2 For Team members:

1) Criminal Prosecution
2) Loss of integrity and reputation
3) Unemployable in senior positions within the financial sector
4) Payment of significant fines or imprisonment, or both
5) Disciplinary action by JMMB (including dismissal)

Table of Major Offences including Fines and Penalties

OFFENCE	**COMPANY INDIV.**	**SANCTIONS**
Engaging in a transaction that involves criminal property	INDIV.	Up to 5 years in jail &/or J$3M (RM Court); Up to 20 years in Jail &/or unlimited fines (Circuit Court)
	COMPANY	Fine up to J$5M (RM Court Unlimited fine (Circuit Court)
Aiding another in Money Laundering	INDIV	Up to 5 years in jail &/or J$3M (RM Court); Up to 20 years in Jail &/or unlimited fines (Circuit Court)
	COMPANY	Fine up to J$3M (RM Court) Unlimited fine (Circuit Court)
"Tipping off" unauthorized persons about Monitoring Orders	INDIV	Up to 3 years in jail and/or a fine of up to $200,000 (RM Court)
	COMPANY	Fine up to J$600,000 (RM Court)
"Tipping off" unauthorized persons about money laundering reports and/or money laundering investigation	INDIV.	Up to 1 year in jail &/or a fine up to J$1M (RM Court) Fine and/or imprisonment for a term not exceeding 10 years (Circuit Court)
Failure to file suspicious or unusual activity reports with the FID	INDIV.	Up to 1 year in jail or up to a fine of J$1,000,000 (RM Court) Fine and/or imprisonment for a

OFFENCE	**COMPANY INDIV.**	**SANCTIONS**
		term not exceeding 10 years (Circuit Court)
Consent given by JMMB Compliance Manager to a prohibited act without the consent of the Designated Authority	INDIV	Up to 1 year in jail and/or fine of up to JJ$1M (RM Court) Fine and/or jail for a term not exceeding five years
Failure to carry out identification, record keeping and internal communications procedures required by law	INDIV.	A fine of up to J$5mil (Parish Court) Fine (Circuit Court)
Failure to file Threshold Transaction Reports (TTR) with FID; Breach of duty of non-disclosure; Failure to comply with directions of the FID re TTRs	COMPANY	A fine of up to J$400,000 (RM Court)
Contravening a Monitoring Order, or providing false or misleading information	COMPANY	A fine of up to J$1M (RM Court)
Failure without reasonable excuse to comply to a Client Information Order	COMPANY	Fine not exceeding J$1M (RM Court).
Failure by the Financial Institution to comply with an	COMPANY	Fine of not less than J$250,000 nor more than J$1M for each

OFFENCE	**COMPANY INDIV.**	**SANCTIONS**
order from the RM Court to pay money held on an account to the Asset Recovery Agency		day that the offence continues.
Providing false or misleading information in purported compliance with a Client Information Order	COMPANY	Fine not exceeding J$1M (RM Court) Unlimited fine (Circuit Court)
Failure to implement controls to detect & prevent laundering	COMPANY INDIV.	A fine of up to J$5mil (Parish Court) Fine (Circuit Court) J$3mil and/or maximum 3 years imprisonment (Parish Court) Fine or maximum 20 years imprisonment (Circuit Court)
Failure to retain records pertaining to electronic funds transfers	COMPANY INDIV.	A fine of up to J$5mil (Parish Court) Fine (Circuit Court) J$3mil and/or maximum 3 years imprisonment (Parish Court) Fine or maximum 20 years imprisonment (Circuit Court)
Failure to establish the necessary AML/CFT standards in overseas branches	COMPANY	A fine of up to J$5mil (Parish Court) Fine (Circuit Court)

OFFENCE	**COMPANY INDIV.**	**SANCTIONS**
	INDIV.	J$3mil and/or maximum 3 years imprisonment (Parish Court) Fine or maximum 20 years imprisonment (Circuit Court)
Failure to designate a Compliance Officer with required functions	COMPANY	A fine of up to J$400,000 (RM Court)
Disclosure of information relating to proposed actions of the Designated Authority (DPP) relating to investigation on a terrorism offence	INDIV. COMPANY	Up to 2 years in jail &/or a fine up to J$2M Up to a fine of J$6M
Engaging in Terrorist Financing including conspiracies or attempting to commit, aid, abet, procure or counsel	INDIV COMPANY	Up to 5 years in jail &/or fine up to J$1M Fine up to J$3M
Directly or indirectly collect property, provide or invite a person to provide or make available, facilitate or carry out terrorist activity using property directly or indirectly	INDIV. COMPANY	Life Imprisonment Unlimited Fine
Disclosure of information relating to actions or proposed	INDIV.	Up to 2 years in jail &/or fines up to J$2M

OFFENCE	**COMPANY INDIV.**	**SANCTIONS**
actions of DPP relating to investigations being conducted or about to be conducted unless to an attorney-at-law for advice	COMPANY	Fine up to J$6M
Transportation of or causing the transportation of cash into and out of Jamaica in excess of US$10,000 without making the requisite report to the designated authority		Up to 3 months in Jails &/or fine up to J$10,000 (RM Court)
Failing to keep records of the securities in which a dealer, investment advisor or their representatives have an interest		Up to $2M &/or imprisonment for up to 2 years.
Transacting business in cash over JA$1M		Fine not exceeding JA$3M &/or three (3) years or less in prison

FATCA

OFFENCE	**COMPANY INDIV.**	**SANCTIONS**
Non-compliance with FATCA	INDIV. COMPANY	• 30% withholding on JMMB • $10,000 for each failure to set out a payment in a return • 10,000 for each failure to set out a payment accurately in a return • $500,000 or less if inaccurate information is submitted • $500,000 if inaccurate information is submitted as a result of an inadvertent failure to comply with the regulations

APPENDIX V – FORMS FOR REPORTING

The submission of Suspicious Activity Report (SAR), Suspicious Transaction Report (STR) and Threshold Transaction Report (TTR) are done via the Financial Investigations Division's (FID) web portal, goAML at https://goaml.fid.gov.jm/repprd/Home

Unusual Transaction Report

THE JMMB GROUP

UNUSUAL TRANSACTION REPORT (UTR)

Reference # .....

☐ Initial Report ☐ Corrected Report ☐ Supplemental Report

....
Report Date Last Report Date (for Corrected or Supplemental Reports)

Kindly provide on the following details on the individual(s) who conducted the transaction(s) if known:

Name	**Universal Client Number**
Date of Birth	**Residential Address**
Contact Number(s)	**TRN**
ID Type, Number & Expiry Date	**Occupation**

Transaction Details (where applicable or known)

Date (DD/MM/YYYY) & Time	
Transaction Type	☐ Investment/Deposit ☐ Encashment/Withdrawal ☐ Cambio/FX ☐ Wire Transfer ☐ Remittance ☐ Insurance Brokerage ☐ Other .....
Currency & Amount	☐ JA$ ☐ US$ ☐ GBP£ ☐ CND$ ☐ Euro€ .....
Source of Funds	
Account(s) Affected	

Why did you deem the transaction unusual (please add sheets if needed)?

.....

.....

.....

.....

Note: It is an offence to advise the client or anyone else of your report

THE JMMB GROUP

Client Details - kindly provide details on the client(s) on the account

Primary Client on Account **UCIN #**	Name ..... Date of Birth ..... Address ..... Nationality ..... Occupation ..... ID Type ..... ID # ..... Expiry Date ..... TRN .....
Joint Account Holder **UCIN #**	Name ..... Date of Birth ..... Address ..... Nationality ..... Occupation ..... ID Type ..... ID # ..... Expiry Date ..... TRN .....
Joint Account Holder **UCIN #**	Name ..... Date of Birth ..... Address ..... Nationality ..... Occupation ..... ID Type ..... ID # ..... Expiry Date ..... TRN .....

....
Prepared by Signature

....
Date Branch/Department

TO BE COMPLETED BY COMPLIANCE TEAM ONLY

Reviewed by (Name) ..... **Title** .....

Signature ..... **Date** .....

Comments .....

.....

12.5 GLOSSORY

Customer Name	(a) in the case of a natural person, the official name recorded at birth or recorded in the records of the Deputy Keeper of the Records and verified by sight of the official identification document; (b) in the case of a legal person, the name in which the business is incorporated or established, and verified by sight of the certificate of incorporation or certificate of Registration of Business Name.
Known Employer	Includes: (a) in the case of a business, one that is registered on the Jamaica Stock Exchange; or a micro, small or medium enterprise (MSME) that is either licensed to operate or, if no such regime exists, one which is required to be registered with a government body or agency or statutory body pursuant in order to operate and is so registered; (b) a financial institution as defined in these Guidance Notes; (c) a financial institution which is registered with or licensed by the Financial Services Commission; or (d) an employer within the public sector. Public sector for the purposes of these Guidance Notes means the Central Government or a public body89 as defined in the Financial Administration and Act.

Long Standing Customer	means a customer with which: (a) a business relationship is held by the financial institution and in respect of which, such relationship was established prior to the 29th day of March, 2007; and (b) in respect of which there has been no change in the risk profile of that customer"
Repeat Customer	means a person who transacts business of US$250 and over or the equivalent amount in any other currency more than once with the financial institution or any of its branches. This must be extended to transactions conducted within a three month period with subsidiaries of financial institutions or other parties to the financial institution or affiliates where the circumstances or the risk profile of the transacting customer warrants this to be done;
Senior Manager	In relation to: (a) a body corporate, means an executive director, a managing director, a chief executive officer, a chief financial officer, the nominated officer, a manager, a senior officer and the company secretary or such other person by whatever name called, who undertakes duties or has responsibilities akin to these positions; (b) any other legal arrangement, includes an individual whose function, by whatever title used, involves functioning as an executive director, a managing director, a chief executive officer, chief financial officer, a nominated officer, a manager or a company secretary or such other function by whatever name called which is akin or equivalent to these functions;

Significant Transaction	Means a transaction undertaken by a financial institution in respect of a customer, which varies substantially in value and/or in amount of business conducted or number of transactions normally undertaken by that customer or in relation to the account/(s) involved. For instance: (a) an account ordinarily involving low value JMD transactions suddenly being used for mid-to-high value transactions in JMD or foreign currency; (b) a relationship that is normally related to banking activities for a corporate customer is used to finance or cover personal expenses or conduct personal banking activities; (c) or deposit and withdrawal activities consistent with a standard personal savings account becomes more consistent with those indicative of flows generated from and/or expenses associated with commercial activity
Critical Transactions	The Bank of Jamaica considers the following to be critical transactions: (a) Transactions effectively amounting to the opening of accounts and/or closing of accounts; (b) Transactions that are assessed as 'high risk' or which are described in the AML/CFT laws as falling in the category of 'high risk'

Team Member Declaration

I _____ have read and fully understand this document and I will

(NAME OF TEAM MEMBER)

abide by all the conditions set forth in this policy statement.

Dated the _____day of _____20

Signed by: _____

Team Member