DB INVEST LIMITED

AML Procedures Manual

Update 10th May 2024

Contents

1.0. Statement

This document describes DB Invest Limited ("the Company") policy and commitment to the detection and prevention of any money-laundering or terrorism financing activity within the products and services offered by the Company.

We will respond to Law Agencies and Other Financial Institutions request about suspicious accounts or transactions by reporting the identity of the specified individual or organization, the account number, all identifying information provided by the account holder when the account was established, and the date and type of transaction.

1.1. Notice to Customers

The company will provide notice to customers that it is requesting information from them to verify their identities, as required by the applicable law. According to the current legislation, the company does not share information concerning the anti-money laundering measures taken by the company with its customers or other individuals.

1.2. Scope

This policy applies to all company officers, employees, appointed contractors, agents, products and services offered by the Company. All business units within the company will cooperate to create a cohesive effort in the fight against money laundering. Each business unit has implemented risk-based procedures reasonably expected to detect and prevent the reporting of transactions. All efforts exerted will be documented and retained.

The AML Compliance Officer is responsible for initiating Suspicious Activity Reports ("SARs") or other required reporting to the appropriate law enforcement or regulatory agencies. Any contacts by law enforcement or regulatory agencies related to the Policy shall be directed to the AML Compliance Officer.

1.3. Definition

Money Laundering is a process intended to mask the benefits derived from serious offenses or criminal conduct as described under the Anti-Money Laundering Act, so that they appear to have originated from a legitimate source. This includes all procedures to change, obscure or conceal the beneficial ownership or audit trail of illegally obtained money or valuables.

Money laundering is also used to hide the link between those who finance terrorism and those who commit terrorist acts. Financing of terrorism can be defined as the willful provision or collection, by any means, directly or indirectly, of funds with the intention that the funds

should be used, or in the knowledge that they are to be used, to facilitate or carry out terrorist acts.

Generally, the process of money laundering comprises three stages, during which there may be numerous transactions that could alert the company to the money laundering activity:

a) Placement - the physical disposal of cash proceeds derived from illegal activity. The aim is to remove cash from the location of acquisition to avoid detection. Smurfing – a form of Placement where the launderer makes many small cash deposits instead of a large one to evade local regulatory reporting requirement applicable to cash transactions.
b) Layering - separating illicit proceeds from their source by creating complex layers of financial transactions (multiple transfers of funds among financial institutions, early surrender of an annuity without regarding to penalties, etc.) Designed to disguise the audit trial and provide anonymity.
c) Integration - the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds. It is the final stage and the process at which the money is integrated into the legitimate economic and financial systems and is assimilated with all other assets in the system. Integration of laundered money into the economy is accomplished by making it appear to have been legally earned.

1.4. Compliance and MLRO

As per section 15(1) (a-e) of the Anti-Money Laundering Act 2006, the company will

a. appoint a compliance and reporting officer who shall be responsible for ensuring the company's compliance with the provisions of the Act;
b. the compliance and reporting officer appointed pursuant to this section will:
    i. be a senior officer with the necessary qualifications and experience and able to respond adequately to enquiries relating to the company and the conduct of its business;
    ii. be responsible for establishing and maintaining such a manual of compliance
    iii. be responsible for ensuring that company's staff comply with the provisions of the Act and any other law relating to money laundering or

financing of terrorism and the provisions of any manual of compliance procedures established; and

iv. act as the liaison officer between the company and the supervising authority and the FIU in matters relating to compliance with the provisions the Act and any other law with respect to money laundering or financing of terrorism;

1.5. Our Approach - Adoption of a Risk-Based Approach

Country Risk: The Company will be cautious of the customer's country origin.

In conjunction with other risk factors, country origin provides useful information as to potential money laundering risks. Factors that may result in a determination that a country poses a heightened risk include:

a) Countries subject to sanctions, embargoes or similar measures.
b) Countries identified by the Financial Action Task Force as non-cooperative in the fight against money-laundering or identified by credible sources as lacking appropriate money laundering laws and regulations.

Customer Risk: There is no universal consensus as to which customers pose a high risk, but the below listed characteristics of customers have been identified with potentially heightened money laundering risks:

a) Armament manufacturers;
b) Cash intensive business;
c) Unregulated charities and other unregulated "non-profit" organizations

Before accepting a potential client, KYC, name screening and due diligence procedures are followed, by examining factors such as customers' background, country of origin, public or high-profile position, linked accounts, business activities or other risk indicators.

Know Your Client and Due Diligence

Before opening an account, we shall see to it that satisfactory and competent evidence is properly obtained on the identity of their customers and that effective procedures have been applied for such verification especially on new customers. Customer Account Information Form (CAIF) is kept for the customers , inclusive of performing name screening using Shufti Pro.

Due diligence must be exercised to prevent the use of the Company as instrument for money laundering. The company implements the following procedures to become aware when it is being requested to "launder money":

a) Customer identification: The company will take all reasonable steps (exercise "due diligence ") to establish, to their satisfaction, the true and full identity of each client inclusive of name screening, and of each client's source of wealth, financial situation and investment. Due diligence is essential for an individual with a high net worth whose source of funds is unclear. We will ensure that we are able to "know" at all times the identity of the persons with whom we are dealing.
b) Customer's suspicious activity: If there are any suspicions about the activities (dealings, money transfers etc.) of an existing or potential customer, they should be reported immediately to the Compliance Officer, who will:
    i receive reports of suspicious activity from the Company's personnel
    ii coordinate required AML reviews/meetings with appropriate staff
    iii gather all relevant business information to evaluate and investigate suspicious activity
    iv determine whether the activity warrants reporting to senior management
    v design and implement training programs as required by this policy
c) Employees are prohibited from disclosing to a client or any other person that information has been passed to the Compliance Officer, management or the regulatory authorities
d) To ensure compliance with this requirement, all personnel will be required to sign a statement on breach of confidentiality provision of the AML.

The company can be exposed to reputational risk and should therefore apply enhanced due diligence to such operations. Private accounts, which by nature involve a large measure of confidentiality, can be opened in the name of an individual, a commercial business, a trust, an intermediary or a personalized investment company. In each case reputational risk may arise if the company does not diligently follow established KYC procedures.

All new clients and new accounts are approved by at least one person, the Compliance officer. In case of a new high-risk customer, the final decision is taken by the CEO. Particular safeguards have been put in place internally to protect confidentiality of customers and their business, the Company ensures that equivalent scrutiny and monitoring of these customers

and their business is conducted, e.g. it is available to be reviewed by compliance officer and auditors. The following are safeguards put in place to protect confidentiality of customers and their business:

- that employees will be required to sign confidentiality agreements
- that the company will adhere to data protection laws of Seychelles
- that there will be segregation of duties between staff and departments and information will be available to different individuals on a need to know basis
- that the organization has put in place strong IT controls to ensure data safety

Compliance with laws

The company ensures that laws and regulations are adhered to under a business environment of high ethical standards and no service shall be provided to any client where there is good reason that money laundering activities are involved.

Cooperation with Law Enforcement Agencies

Should there be reasonable grounds for suspecting money laundering, we shall fully cooperate with proper law enforcement agencies within the legal constraints relating to customer confidentiality.

Dissemination of policies and procedures

Policies and procedures to prevent possible money laundering activities are properly disseminated to our officers and staff.

1.6. Customer Identification

The identification of customer seeking to open an account with us is an essential part of our KYC process. The company does not enter into any service relationship until the identity of the new customer or the person acting on his/ her behalf (Beneficial Owner) is fully verified. Information must be provided to learn:

i the true Identity of the Customer,

ii the nature of the Customer's Business,

iii the intended Purpose of the Customer's transactions,

The extent and nature of the information depends on the type of applicant (personal, corporate, etc.) and the expected size of the account.

Our customers are subdivided into two major categories:

a) Private customers (natural persons)
b) Corporate customers

Private customers (natural persons):

If the customer is a Natural person and low risk, the following information must be collected:

i True name and/or names used
ii Residence address, city code, telephone number
iii Business address
iv Date and Place of birth

Names should be verified by:

i Valid Passport
ii National ID Card
iii current photo-card driving license

The indicated documents should not be older than 6 months from the filing date.

The current permanent address will be verified by one of the followings:

i Proof of a recent utility bill
ii Customer's tax identification numbers, Social Security number or Government Service and Insurance System number
iii Bank statement
iv Credit card monthly statement

The utility bill, bank statement and credit card statement should not be older than 3 months from the filing date.

The copy of the customer's tax identification numbers, Social Security number or Government Service and Insurance System number should be apostilled in the country of origin.

All documents should be certified by either of the following:

- a judge;
- a magistrate;
- a notary public;
- a barrister-at-law;

- a Solicitor;
- an attorney-at-law; or
- a Commissioner of Oaths.

For each account we shall also make reasonable effort, prior to the settlement of the initial transaction, to obtain the following information to the extent it is applicable to the account:

i Occupation of customer;
ii The customer's investment objective and other related information concerning the customer's financial situation and needs;
iii Annual income, Assets or net worth;

Approval of the Account or "new client" is subject to the following terms and conditions:

i The Customer Account Information Form is filled in completely;
ii Clear photocopy of a valid ID with photo of the client is obtained;
iii Recommendation of client is provided by the Investment Agent;
iv Sufficient background check is conducted by our compliance team

All applications are carefully examined by the compliance officer to ensure that all required information/ documents are gathered. To approve an application, the Compliance officer must verify the following:

i The completeness of the required agreement/identification documents
ii The correctness, authenticity and completeness of the information provided by the applicant
iii The creditworthiness of the applicant, through a database search whenever this deems necessary
iv The probability that the applicant is involved in illegal or criminal activities
v And, reject all applications that do not include all the necessary information

Corporate customers:

Before establishing a business relationship, a company search and/or other commercial inquiries shall be made to ensure that the corporate/other business applicant has not been, or is not in the process of being dissolved, struck off, wound-up or terminated. In the event of doubt as to the identity of the company or its directors, or the business or its partners, a search or inquiry with the relevant Supervising Authority/Regulatory Agency shall be made.

The following relevant documents shall be obtained in respect of corporate/other business applicants:

i Copies of the Certificate of Registration, including Articles of Incorporation or Certificate of Partnership, as appropriate,

ii Copies of the By-Laws and Latest General Information Sheet, which lists the names of directors/partners and principal stockholders, and secondary licenses.

iii The originals or certified copies of any or all of the foregoing documents, where required, should be produced and submitted for verification.

a. Sworn statement as to existence or non-existence of beneficial owners.
b. Appropriate Board of Directors' resolutions and signed application forms or account opening, identifying the authorized signatories or principal officers of the corporation authorized to trade and their authorities and specimen signatures.
c. Board Resolution authorizing the corporation to open the account with the Company.
d. Latest Audited Financial Statements.
e. Where necessary, we may also require additional information about the nature of the business of clients, copies of identification documents of shareholders, directors, officers and all authorized signatories

Enhanced Customer Due Diligence

DB Invest Limited will perform enhanced customer due diligence -

(a) where a higher risk of money laundering or terrorist financing has been identified,
(b) where through supervisory guidance a high risk of money laundering or terrorist financing has been identified;
(c) where a customer or an applicant for business is from a foreign country that has been identified by credible sources as having serious deficiencies in its anti-money laundering or counter terrorist financing regime or a prevalence of corruption;
(d) in relation to correspondent banking relationships,
(e) where the customer or the applicant for business is a political exposed person; or
(f) in the event of any unusual or suspicious activity

High Risk Customers/ Politically Exposed Persons

A PEP is defined in Sec 6 of the AML Regulations as an individual entrusted with a prominent public function in the last three (3) years, and includes any immediate family member or close associate of such an individual. Both local and foreign PEPs are covered by this definition.

The company will have a risk management system in place to determine if an existing customers becomes a PEP and should conduct regular searches and checks for this purpose.

At this point the Company will not be onboarding PEPs. At the point that an existing Client becomes a PEP such client will have their accounts terminated.

The company will search for information from reliable sources including https://www.world-check.com , google search and Shufti Pro. The company will also rely on public information as allowed by the Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism Procedures in determining whether persons are within the definition of „close associates" (for example, partners or joint venturers), and will conduct regular searches and checks for this purpose.

If the customer is a high risk, the company will perform the following procedures

i. adequately identify the person and verify his or her identity as set out in this section;
ii. obtain the approval of senior management before establishing a business relationship with the customer;
iii. take reasonable measures to establish the person's source of wealth and source of property and
iv. conduct regular enhanced monitoring of the business relationship.

KYC procedures for dealings with Medium and High Risk Customers

The following documents shall be requested for customers considered to be high risk

a) Proof of Identification
b) Proof of Address

c) Proof of source of funds
d) Detailed Resume

KYC procedures for dealings with professional intermediaries and/or reseller clients

When dealing with intermediaries or third parties to undertake our obligations to introduce business, we will perform the following procedures:

a) immediately obtain the information required
b) ensure that copies of identification data and other relevant documentation relating to the requirements will be made available to it from the intermediary or the 'third party upon request without delay; and
c) satisfy ourselves that the third party or intermediary is regulated and supervised for, and has measures in place to comply with, the requirements set out in sections 5, 6 and 7 of the Anti-Money Laundering Act 2006.

1.7. Changes to the Customer Status and Operations

The company immediately takes all necessary actions using the identification procedures and measures to provide due diligence, in order to collect the appropriate evidence in cases of:

a) changes to the customer documentation standards, such as:
    i. change of directors/secretary;
    ii. change of registered shareholders and/or actual beneficiaries;
    iii. change of registered office;
    iv. change of trustees;
    v. change of corporate name and/or trade name;
    vi. change of main trading partners and/or significant new business;
b) a material change in the way an account is operated, such as:
    i. change of persons authorized to handle its account;
    ii. request for opening a new account in order to provide new investment services and/or financial instruments;
c) a significant transaction that appears to be unusual and/or significant than the usual type of trade and profile of the client;

1.8. Enhanced Customer Scrutiny and Rejection

Based on the risk, we will analyze any logical inconsistencies in the information or behavior of its customers. If a potential or existing client either refuses to provide the information

described in the above chapters, or appears to have intentionally provided misleading information, a new account will not be opened and, after evaluating the risks involved, will consider closing any existing account. We will also refuse any account which is determined to be "high risk" by the Compliance officer.

1.9. Verification of Customer Identity

The company has implemented an integrated multilevel electronic system of information verification provided by the Customer. This system documents and checks identification details of the Customer, keeps and controls drill through reports of all the transactions.

The following are some counter checks being done by us to verify identity of clients without face to face contact:

i Telephone contact of the applicant at an independently verifiable home or business number;

ii Submission of Income tax return, and also bank statement or any proof of income;

iii Confirmation of address through correspondence or presentation of proof of billing address;

Above procedures should be strictly implemented when opening of accounts via telephone, internet or by mail; especially if the client is just referred by another client or any of the staff. Such requirements should ideally be done prior to executing the initial transaction. For non-residents who seek to procure transactions without face-to-face contact, documents as enumerated above issued by foreign authorities must be submitted.

The company always requires its clients to submit information particularly on the source of funds. If the client states that he/she has a business, some proof of the business documents, like by-laws, Business registration, etc. are requested. Company search on the website for registered companies is done to ensure that the corporate or other business applicant is an existing business entity.

Customer identification and information of existing clients should be updated and/or amended at least once every two (2) years. This refers to change of residential or business address, new identification cards, new passport, additional business information, new business investment/venture, and the like. For any change of information before the said period the company requests a letter or document pertaining to the changes being made.

Bearing in mind the "Know – Your – Customer" principle, we should be in a position of no-doubt or no suspicions that the identities of our clients are questionable after careful evaluation of all identification documents submitted to us. This should be very important where the client is a non-resident and therefore more probing must be done on the purpose of the transaction and the sources of funds, especially if it involves a significant amount, except when such client is a long-established and well-known customer.

Once an account is opened for a client, particular care shall be taken in cases where instructions for transactions on behalf of said client is being made by another person or party, such person or party must be formally authorized by the client account to make such transactions on his/her behalf. The company shall require the necessary documents such as Special Power of Attorney (SPA) or duly signature-verified authorization given by clients; e.g. authorized to place an order; up to what amount; and authorized to get the withdrawal.

We shall establish whether the applicant for business relationship is acting on behalf of another person as trustee, nominee or agent. The Company shall obtain authorized evidence of the identity of such agents (the same documents needed as enumerated above) and authorized signatories, and the nature of their trustee or nominee capacity and duties.

In cases where a potential customer insists for confidentiality reasons, a numbered account may be opened. Confidential numbered accounts should not function as anonymous accounts but they should be subject to exactly the same KYC procedures as all other customer accounts, even if the test is carried out by selected staff. Whereas a numbered account can offer additional protection for the identity of the account-holder, the identity must be known to a sufficient number of staff to operate proper due diligence.

Shell companies are legal entities which have no business substance in their own right but through which financial transactions may be conducted. It is the policy of the company to always be cautious when dealing with these companies as these are often abused by money launderers. In addition to the requirements about corporation, we shall require a Board of Directors' certification as to the purpose(s) of the owners/stockholders in acquiring the shell company. There must be satisfactory evidence of the identities of the beneficial owners bearing in mind the "Know-Your-Customer" principle.

As a policy, we do not allow named account holders to transact for non-account holders and should therefore exercise special care and vigilance. Where transactions involve significant

amounts, the customer should be asked to produce competent evidence of identity including nationality, the purposes of the transaction, and the sources of the funds.

The company will document its verification, including all identifying information provided by the customer, the methods used and results of the verification.

1.10. Monitoring of Customer Activity and Records

The company monitors suspicious and revenue-intensive transactions closely, takes timely, appropriate actions on said transactions and informs the appropriate bodies without undue delay.

The system of monitoring implemented by the company relies both on automated monitoring and, where appropriate, manual monitoring by the staff. A series of status fields have been applied to customer accounts indicating their profile within the system, which assist automated monitoring. We have adopted a regulatory and legally compliant process for suspicious activity reporting that will enable all staff to make a report to the Compliance Officer where they know or suspect that a customer is engaged in money laundering or terrorist financing.

Our staff are trained to monitor a sufficient amount of account activity to permit identification of patterns of unusual size, volume, type of transactions, geographic factors such as whether jurisdictions designated as "non-co-operative" are involved or any of the "red flags" identified below. The company shall look at transactions, including deposits and wire transfer, in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction for that customer. The AML Compliance Officer who will be responsible for this monitoring, will document when and how the transaction is carried out, and will report suspicious activities to the appropriate authorities.

Examples of Red Flags are:

- The customer exhibits unusual concern regarding the Company's compliance with government reporting requirements and AML policy, particularly with respect to his/her identity, type of business and assets, or refuses to reveal any information concerning business activates, or furnishes suspicious identification documents;

- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business strategy;
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect;
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his/her funds and other assets;
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil or regulatory violations;
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs;
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant to provide information, or is otherwise evasive regarding that person or entity;
- The customer has difficulty describing the nature of his/her business or lacks general knowledge of his/her industry;
- The customer attempts to make frequent or large deposits, insists on dealing only in cash equivalents, or asks for exemptions from the Company's policies relating to the deposits of cash and cash equivalents;
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to avoid the government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds;
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers;
- The customer is from, or has accounts in, a country identified as a non-cooperative country by the Financial Action Task Force;
- The customer's account has unexpected or sudden extensive wire activity, especially in accounts that had little or no previous activity;
- The customer's account shows numerous currency or cashier's check transactions aggregating to significant sums;
- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose;

- The customer's account has wire transfer's that have no apparent business purpose to or from a country identified as money laundering risk;
- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or by debit card without any apparent business purpose;
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose;
- The customer makes a fund deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account;
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose;
- The customer requests that a transaction be processed in such a manner to avoid the Company's normal documentation requirements;
- The customer engages in transactions involving certain type of securities, such as penny stocks and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering. (Such transactions may warrant due diligence to ensure the legitimacy of the customer's activity);
- The customer's account shows an unexplained high level of account activity with very low levels of transactions;
- Attempt to borrow maximum cash value of a single premium policy soon after purchase;

When a staff member of the company detects any red flag he/she will investigate further under the direction of the AML Compliance Officer. This may include gathering additional information internally or from third party sources, contacting the appropriate authority or freezing the account.

Additionally, the Compliance Officer will be responsible for ongoing Monitoring including monitoring of records kept on client due diligence information and other relevant records.

In general client accounts and records will be monitored and reviewed as follows:

High risk Clients – Every 6 Months
Medium risk – Every 1 years

Low risk – Every 2 years

1.11. Deposit and Withdrawal Requirements

The company monitors funding from various bank accounts outside of the account holder's home country. In case of bank transfer or transfer from a bank card, the name, indicated during the registration must match the name of the owner of the account/bank card.

The company neither accepts cash deposits nor disburses cash under any circumstances.
The withdrawal process detailed below is structured around strict guidelines to make sure that funds are securely sent back to their originating source and beneficiary:

i. Our customers must complete a withdrawal request containing their correct account information.
ii. All withdrawal forms are submitted to our accounts department for processing. Our Accounts department confirms the account balance, verifies that there are no holds or withdrawal restrictions on the account, and then approves the withdrawal request, pending compliance approval.
iii. Our Accounts department reviews all withdrawal requests, verifying the original funds are withdrawn via the same method of deposit and to the account holder on file. Our accounts department examines the withdrawal request against the customer's deposit history to make sure there is no suspicious activity and verifies the bank account on file.
iv. Withdrawal requests approved are processed by the accounts department and the funds are released to the client.
v. In the event that a withdrawal is flagged for suspicious activity, the withdrawal is placed on hold, pending further investigation by our compliance department.
vi. Our Management will work with the Compliance department to see if further action needed and if any relevant regulatory bodies need to be contacted.

1.12. Record Keeping

Records will be kept for all documents obtained for the purpose of customer identification (KYC policy requirements) and all data of each transaction, as well as other information related to money laundering matters in accordance with the applicable anti-money laundering laws/regulations. That includes files on suspicious activity reports, documentation of AML account monitoring, etc.

Transaction effected via the company can be reconstructed, from which the authorities will be able to compile an audit trail for suspected money laundering, when such a report is made to it. The Company can satisfy within a reasonable time any inquiry or order from the authorities as to disclosure of information, including without limitation whether a particular person is the customer or beneficial owner of transactions conducted through the Company. The following document retention periods will be followed:

i All documents in opening the accounts of clients and records of all their transactions, especially customer identification records, shall be maintained and safely stored for seven (7) years from the dates of transactions.

ii With respect to closed accounts, the records on customer identification, account files and business correspondence, shall be preserved and safely stored for at least seven (7) years from the dates when they were closed.

The following records must be kept:

i Copies of the evidential material of the customer identity.

ii Any non-documentary verification methods or additional methods used to verify.

iii Relevant evidential material and details of all business relations and transactions, including documents for recording transactions in the accounting books (the form and source of funds and/or securities used by the applicant for business; the form and destination of funds paid or delivered to the applicant for business or another person on his behalf; financial transactions carried out by the Company with or for each client or counterparty of the Company.

iv Relevant documents of correspondence with the customers and other persons with whom they keep a business relation.

v Description of how the company resolved all substantive discrepancies noted.

Checking and review of the documents is done by the personnel assigned to verify the accuracy and completeness of the records maintained by the company. It is important that

any material irregularity or documents lacking are noted and reported for immediate correction.

Transaction documents may be retained as originals or copies, on microfilm, or in electronic form, provided that such forms are admissible in court.

If the records relate to on-going investigations or transactions that have been the subject of a disclosure, they shall be retained beyond the stipulated retention period until it is confirmed that the case has been closed and terminated.

1.13. Reporting Requirements

The company shall institute a system for the mandatory reporting of suspicious transactions by appointing a Compliance Officer. Reporting of covered and suspicious transactions must be done by the Compliance Officer within five (5) working days.

Employees, Agents, Compliance Officer, and/or directors shall not warn their customers when information relating to them is being reported to the Authorities.

The company shall register or maintain a complete file on all covered and suspicious transactions that have been brought to the attention of the Compliance Officer. The register shall contain details of:

i the date on which the report is made,
ii the person who made the report to the Compliance Officer,
iii information sufficient to identify the relevant papers related to said reports.

The Financial Intelligence Unit (FIU) has a platform where the AML Compliance Officer can submit SARs as above. In general, the name and address of the client as well as the descriptopn and nature of the transaction will be reported as to the reason as to why the transaction and/or client is believed to be Suspicious.

Upon discovery of any suspicious activity from proof of funds and other checks the suspected account will be cancelled and the relationship with the client terminated.

1.14. Internal Control and Procedures

As a general internal control procedure, directors, officers, agents and staff of the company shall report any knowledge or suspicion of money laundering activity to the Compliance

Officer. The report should be formally transmitted either in hard copy report, memoranda or note, or via electronic means (inter-office email). Use of external emails in transmitting the report is prohibited. Ensure no one else is provided a copy (including blind copies). Failure to comply with such requirement exposes the reporting personnel to breach of confidentiality in violation of the Anti-Money Laundering Act.

In line with this requirement, all personnel will be required to sign a statement on breach of confidentiality provision of the AML Act. A copy of this signed statement will be filed together with the personnel file.

After thorough evaluation and reasonable belief that there is really a basis for suspicion of money laundering, Compliance Officer shall maintain a register of all reports made to the authorities as well as all reports made by the staff of the Company relative to suspicious transactions, whether or not such were reported to the Authorities.

Notwithstanding the duties of the Compliance Officer as reporting officer, the ultimate responsibility for proper supervision, reporting and compliance with the Anti-Money Laundering Act and its implementing Rules and Regulations, shall rest with the company and its Board of Directors.

1.15. Training of the Staff

The company provides the necessary training, as well as orientation to its Agents and Compliance Officer. The Company disseminates to the staff the new procedures and guidelines needed in combating money laundering. The officers and staff are sent to orientations, training and seminars being offered by the regulatory bodies.

The company also educate staff in the "Know Your Customer" requirements on the prevention and detection of money laundering. Staff will therefore be trained in the true identity of customers and the type of business relationship being established.

The company shall determine the extent of training/orientation of its personnel with the priority being given to the Compliance Officer who would be directly exposed to situations involving money laundering activities. Scope of training is on the following:

i Provisions of the AML Act
ii The Company's AML Policy
iii The Company's Internal Supervision, Control, and Compliance Procedures
iv Updates and changes on the AML Act
v Updates and changes on Internal Supervision, Control, and Compliance Procedures

Refresher training or orientations shall be made from time to time to constantly remind key staff of their responsibilities or if there are changes in the laws and rules in money laundering.

The Company will ensure that the Staff are trained at the minimum on an annual basis as well as each and every time there are new laws impacting the Company or changes to existing laws and legal requirements.

1.16. Test of the AML Policy

We will hire an independent, qualified party to provide an annual independent audit of our AML policies and procedures, and the compliance with said procedures. The Company will perform written follow-up to ensure that any deficiencies noted during its annual review are addressed and corrected.

The Company will confirm with its AML audit firm that their audit program includes the following:

i. Audit objectives and scope of the exam;
ii. Any recommendations on improving the AML program;
iii. A discussion of any noted deficiencies and an action plan to be implemented by management to address these deficiencies;
iv. An overall opinion of the adequacy of the Company's AML program.

A report of the independent review shall be addressed to senior management with a copy being maintained by the Company's AML Compliance Officer.

Compliance Officer, DB Invest Limited
Bernard Domingue

10/05/2024

Director, DB Invest Limited
Gennaro Lanza

10/05/2024