

Financial Intelligence and Anti-Money Laundering Regulations 2018

GN 108/2018

Government Gazette of Mauritius No. 88 of 28 September 2018

THE FINANCIAL INTELLIGENCE AND ANTI-MONEY LAUNDERING ACT

Regulations made by the Minister under sections 17C, 170, 17E and 35 of the Financial Intelligence and Anti-Money Laundering Act

1. These regulations may be cited as the Financial Intelligence and Anti-Money Laundering Regulations 2018.

2. In these regulations —

“Act” means the Financial Intelligence and Anti-Money Laundering Act;

“accurate” means information that has been verified for accuracy;

“applicant for business” means a person who seeks to establish a business relationship, or carries out an occasional transaction, with a reporting person;

“beneficial owner” —

(a) means the natural person —

(i) who ultimately owns or controls a customer; or

(ii) on whose behalf a transaction is being conducted; and

(b) includes those natural persons who exercise ultimate control over a legal person or

arrangement and such other persons as specified in regulations 6 and 7;

“competent authorities” —

- (a) means a public authority to which responsibility to combat money laundering or terrorist financing is designated; and
- (b) includes a supervisory authority, regulatory body and an investigatory authority;

“consolidated supervision”, in relation to a financial services group, means supervision of the group by a regulatory body on the basis of the totality of its business, wherever conducted;

“core principles” means the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors;

“correspondent banking” means the provision of banking services by one bank, the correspondent bank, or the correspondent bank, to another bank, or the respondent bank;

“cross border wire transfer” —

- (a) means any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries; and
- (b) includes any chain of wire transfer in which at least one of the financial institutions involved is located in a different country;

“customer” means a natural person or a legal person or a legal arrangement for whom a transaction or account is arranged, opened or undertaken and includes —

- (a) a signatory to a transaction or account;
- (b) any person to whom an account or rights or obligations under a transaction have been assigned or transferred;

(c) any person who is authorised to conduct a transaction or control an account;

(d) any person who attempts to take any action referred to above;

(e) an applicant for business;

“domestic wire transfers” means any wire transfer where the ordering financial institution and beneficiary financial institution are located in Mauritius;

“financial group” means a group that consists of a parent company or of any other entity exercising control and coordinating functions over the rest of the group for the application of group supervision under the core principles, together with branches or subsidiaries that are subject to Anti-Money Laundering or the Combatting the Financing of Terrorism policies and procedures at the group level;

“financial services group” means a group of companies whose activities include to a significant extent activities that are, or if carried on in Mauritius would be, activities regulated by the Bank of Mauritius or the Financial Services Commission;

“identification data” means reliable, independent source documents, data or information;

“international organisations” means entities established by formal political agreements between their member States that have the status of international treaties, whose existence is recognised by law in their member countries, and they are not treated as resident institutional units of the countries in which they are located;

“MVTs provider” means a body corporate licensed by the Bank of Mauritius to carry on the business of money or value transfer services;

“occasional transaction” means any transaction carried out other than in the course of a business relationship;

“originator” means the account holder who allows the wire transfer from that account, or where there is no account, the person who places the order with the ordering financial institution to perform the wire transfer;

“payable-through account” means a correspondent account that is used directly by third parties to transact business on their own behalf;

“physical presence” —

(a) means meaningful mind and management located within a country; and

(b) excludes the existence of simply a local agent or low level staff

“politically exposed person” or “PEP” —

(a) means a foreign PEP, a domestic PEP and an international organisation PEP; and

(b) for the purposes of this definition —

“domestic PEP” means a natural person who is or has been entrusted domestically with prominent public functions in Mauritius and includes the Head of State and of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee;

“foreign PEPs” means a natural person who is or has been entrusted with prominent public functions by a foreign country, including Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee;

“international organisation PEP” means a person who is or has been entrusted with a prominent function by an international organisation and includes members of senior management such as directors, deputy directors and members of the board or equivalent functions, or individuals who have been entrusted with equivalent functions, including directors, deputy directors and members of the board or equivalent functions and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee;

“reasonable measures” means appropriate measures which are commensurate with the money laundering or terrorist financing risks;

“satisfied” where reference is made to a reporting person being satisfied as to a matter means the reporting person shall be able to justify his assessment to competent authorities, including a regulatory body, a supervisory authority, an investigatory body or the FIU;

“senior management” means an officer or employee with sufficient knowledge of the institution’s money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors;

“shell bank” means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision;

“wire transfer” means any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.

Amended by [\[GN No. 122 of 2018\]](#); [\[Act No. 9 of 2019\]](#)

3. (1) A reporting person shall —

- (a) identify his customer whether permanent or occasional and verify the identity of his customer using reliable,

independent source documents, data or information, including, where available, electronic identification means, or any other secure, remote or electronic identification process as may be specified by the relevant regulatory body or supervisory authority;

- (b) verify that any person purporting to act on behalf of a customer is so authorised, and shall identify and verify the identity of that person;

- (c) identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using relevant information or data obtained from a reliable source such that the reporting person is satisfied that he knows who the beneficial owner is;

- (d) understand and obtain adequate and relevant information on the purpose and intended nature of a business relationship or occasional transaction;

- (e) conduct ongoing monitoring of a business relationship, including —

- (i) scrutiny of transactions undertaken throughout the course of the relationship, including, where necessary, the source of funds, to ensure that the transactions are consistent with his knowledge of the customer and the business and risk profile of the customer;

- (ii) ensuring that documents data or information collected under the Customer Due Diligence (CDD) process are kept up to date and relevant by undertaking reviews of existing records, in particular for higher risk categories of customers.

(2) Subject to paragraph (3), where there is a suspicion of money laundering, terrorism financing or proliferation financing, the reporting person shall, notwithstanding any applicable thresholds, undertake CDD measures in accordance with this regulation.

(3) Where a reporting person suspects money laundering, terrorism financing or

proliferation financing, and he reasonably believes that performing the CDD process, may tip-off the customer, he shall not pursue the CDD process and shall file a suspicious transaction report under section 14 of the Act.

(4) A suspicious transaction report under paragraph (3) shall specify the reasons for not pursuing the CDD process.

4. (1) For a customer who is a natural person, a reporting person shall obtain and verify —

(a) the full legal and any other names, including, marital name, former legal name or alias;

(b) the date and place of birth;

(c) the nationality;

(d) the current and permanent address; and

(e) such other information as may be specified by a relevant supervisory authority or regulatory body.

(2) For the purposes of paragraph (1), documentary evidence as may be specified by a relevant regulatory body or supervisory authority shall be used for the purposes of verification of identity requirement.

5. (1) Where the customer is a legal person or legal arrangement, a reporting person shall —

(a) with respect to the customer, understand and document —

(i) the nature of his business; and

(ii) his ownership and control structure;

(b) identify the customer and verify his identity by obtaining the following information —

- (i) name, legal form and proof of existence;
- (ii) powers that regulate and bind the customer;
- (iii) names of the relevant persons having a senior management position in the legal person or arrangement; and
- (iv) the address of the registered office and, if different, a principal place of business.

(2) In this regulation –

“senior management” means senior managing official.

Amended by [\[Act No. 9 of 2019\]](#)

6. (1) Where the customer is a legal person, the reporting person shall identify and take reasonable measures to verify the identity of beneficial owners by obtaining information on —

- (a) the identity of all the natural persons who ultimately have a controlling ownership interest in the legal person;
- (b) where there is doubt under subparagraph (a) as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control of the legal person through other means as may be specified by relevant regulatory body or supervisory authority; and
- (c) where no natural person is identified under subparagraph (a) or (b), the identity of the natural person who holds the position of senior managing official.

(2) A reporting person shall keep records of the actions taken under paragraph (1) as well as any difficulties encountered during the verification process.

Amended by [\[GN No. 122 of 2018\]](#); [\[Act No. 9 of 2019\]](#)

7. For customers that are legal arrangements, the reporting person shall identify and take reasonable measures to verify the identity of beneficial owners by obtaining information —

- (a) for trusts, on the identity of the settlor, the trustee, the beneficiaries or class of beneficiaries, and where applicable, the protector or the enforcer, and any other natural person exercising ultimate effective control over the trust, including through a chain of control or ownership;
- (b) for other types of legal arrangements, on the identity of the persons in equivalent or similar positions.

8. (1) In addition to the CDD measures for a customer and a beneficial owner, a reporting person shall conduct CDD measures under this regulation on the beneficiary of life insurance and other investment related insurance policies as soon as the beneficiary is identified or designated.

(2) For a beneficiary that is identified as a specifically named natural or legal person or legal arrangement, the reporting person shall take the name of that person.

(3) For a beneficiary that is designated by characteristics or class, or by other means, the reporting person shall obtain sufficient information concerning the beneficiaries to satisfy the life or investment-related insurance business that he will be able to establish the identity of the beneficiary at the time of the payout.

(4) In all the above cases, the reporting person shall verify the identity of the beneficiary at the time of the payout.

(5) Where a reporting person is unable to comply with this regulation, it shall make a suspicious transaction report under section 14 of the Act.

9. (1) Subject to paragraph (3), a reporting person shall verify the identity of the customer and

beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers.

(2) Where doubts exist about the veracity or adequacy of previously obtained customer identification information, the reporting person shall identify and verify the identity of the customer and beneficial owner before the customer may conduct any further business.

(3) Subject to paragraph (4), a reporting person may be allowed by the relevant supervisory authority or regulatory body to complete the verification of the identity of the customer and beneficial owner after the establishment of the business relationship, provided that —

- (a) this is essential not to interrupt the normal conduct of business;
- (b) the verification of identity occurs as soon as reasonably practicable;
and
- (c) the money laundering and terrorism financing risks are effectively managed by the reporting person.

(4) Where the reporting person is allowed to establish the business relationship before the completion of the verification of identity of the customer and beneficial owner, he shall adopt and implement risk management procedures concerning the conditions under which a customer may utilise the business relationship prior to verification.

Amended by [\[GN No. 122 of 2018\]](#)

10. In determining when to take CDD measures in relation to existing customers, a reporting person shall take into account, among other things —

- (a) any indication that the identity of the customer or the beneficial owner, has changed;
- (b) any transactions which are not reasonably consistent with his knowledge of the customer;

- (c) any change in the purpose or intended nature of his relationship with the customer;
- (d) any other matter which might affect his assessment of the money laundering, terrorist financing or proliferation financing risk in relation to the customer.

11. (1) Notwithstanding regulations 4, 5 and 6, a reporting person may apply simplified CDD measures where lower risks have been identified and the simplified CDD measures shall be commensurate with the lower risk factors and in accordance with any guidelines issued by a regulatory body or supervisory authority.

(2) Where a reporting person determines that there is a low level of risk, he shall ensure that the low risk identified is consistent with the findings of the national risk assessment or any risk assessment of his supervisory authority or regulatory body, whichever is most recently issued.

(3) Simplified CDD shall not apply where, a reporting person knows, suspects, or has reasonable grounds for knowing or suspecting that a customer or an applicant for business is engaged in money laundering or terrorism financing or that the transaction being conducted by the customer or applicant for business is being carried out on behalf of another person engaged in money laundering or terrorist financing.

(4) For the purpose of this regulation —
“national risk assessment” means the report issued under section 19D(2) of the Act.

12. (1) A reporting person shall perform enhanced CDD —

- (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 high risk third country;

- (d) in relation to correspondent banking relationships, pursuant to regulation 16;
- (e) subject to regulation 15, where the customer or the applicant for business is a political exposed person;
- (f) where a reporting person discovers that a customer has provided false or stolen identification documentation or information and the reporting person proposes to continue to deal with that customer;
- (g) in the event of any unusual or suspicious activity.

(2) Enhanced CDD measures that may be applied for higher risk business relationships include —

- (a) obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of the customer and the beneficial owner;
- (b) obtaining additional information on the intended nature of the business relationship;
- (c) obtaining information on the source of funds or source of wealth of the customer;
- (d) obtaining information on the reasons for intended or performed transactions;
- (e) obtaining the approval of senior management to commence or continue the business relationship;
- (f) conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;

(g) requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

(3) Where a reporting person is unable to perform enhanced CDD where required under these regulations, he shall terminate the business relationship and shall file a suspicious transaction report under section 14 of the Act.

(4) A reporting person shall include the beneficiary of a life insurance policy as a relevant risk factor when determining whether enhanced CDD measures are required.

(5) Where a reporting person determines that the beneficiary who is a legal person or a legal arrangement presents a higher risk, the reporting person shall take enhanced due diligence measures which shall include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary at the time of payout.

13. Where a reporting person is unable to comply with relevant CDD measures under these regulations, he shall —

- (a) not open the account, commence the business relationship or perform a transaction;
or
- (b) terminate the business relationship; and
- (c) in relation to the customer, file a suspicious transaction report under section 14 of the Act.

14. (1) A reporting person shall keep and maintain all necessary records relating to transactions in such a form which enables the prompt reconstruction of each individual transaction.

(2) For the purpose of paragraph (1), where a reporting person is responding to a request under section 13(2) of the Act or to a request from any relevant regulatory body or supervisory authority, it shall provide for each transaction record —

- (a) the full name of the party making a payment; and
- (b) the full name of the party receiving a payment.

(3) A reporting person shall ensure that all CDD information and transaction records are kept in such a manner that they are swiftly made available to the FIU or any relevant regulatory body or supervisory authority or the other competent authority upon request.

Amended by [\[GN No. 122 of 2018\]](#)

15. (1) A reporting person shall in relation to a foreign PEP, whether as customer or beneficial owner, in addition to performing the CDD measures under these regulations —

- (a) put in place and maintain appropriate risk management systems to determine whether the customer or beneficial owner is a PEP;
- (b) obtain senior management approval before establishing or continuing, for existing customers, such business relationships;
- (c) take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and
- (d) conduct enhanced ongoing monitoring on that relationship.

(2) A reporting person shall, in relation to domestic PEPs or an international organisation PEP, in addition to performing the CDD measures required under these regulations —

- (a) take reasonable measures to determine whether a customer or the beneficial owner is such a person; and
- (b) in cases when there is higher risk business relationship with a domestic PEP or an international organization PEP, adopt the measures in paragraphs (l)(b) to (d).

(3) A reporting person shall apply the relevant requirements of paragraphs (1) and (2) to family members or close associates of all types of PEP.

(4) A reporting person shall, in relation to life insurance policies, at any time but before the time of payout, take reasonable measures to determine whether the beneficiaries or the beneficial owner of the beneficiary, are PEPs, provided that where higher risks are identified, the reporting person shall —

(a) inform senior management before the payout of the policy proceeds;

(b) conduct enhanced scrutiny on the whole business relationship with the policyholder; and

(c) consider making a suspicious transaction report.

(5) For the purpose of this regulation —

“close associates” —

(a) means an individual who is closely connected to a PEP, either socially or professionally; and

(b) includes any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee;

“family members” —

(a) means an individual who is related to a PEP either directly through consanguinity, or through marriage or similar civil forms of partnership; and

(b) includes any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

Amended by [\[GN No. 122 of 2018\]](#)

16. (1) In relation to cross border correspondent banking and other similar relationships, a reporting person shall, in addition to the CDD measures —

- (a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business;
- (b) determine from publicly available information the reputation of the respondent institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;
- (c) assess the respondent institution's anti-money laundering and combating the financing of terrorism controls;
- (d) obtain approval from senior management before establishing new correspondent relationships;
- (e) clearly understand and document the respective responsibilities of each institution.

(2) With respect to payable-through accounts, a reporting person shall be satisfied that the respondent bank —

- (a) has performed CDD obligations on its customers having direct access to accounts of the correspondent bank; and
- (b) is able to provide relevant CDD information upon request to the correspondent bank.

17. (1) A reporting person shall not enter into or continue a business relationship or occasional transaction with a shell bank.

(2) A reporting person shall take adequate measures to ensure that he does not enter into or continue a business relationship or occasional transaction with a respondent institution that permits its accounts to be used by a shell bank.

18. A MVTs provider shall —

(a) maintain a list of all its agents or subagents which shall be provided —

(i) to the FIU or to the relevant supervisory or competent authority upon request;

(ii) to competent authorities in countries in which its agent operates;

(b) include agents in their programs for combating money laundering and terrorism financing and monitor them for compliance with these programs.

Amended by [\[GN No. 122 of 2018\]](#)

19. (1) A reporting person shall identify and assess the money laundering and terrorism financing risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

(2) A reporting person shall —

(a) undertake the risk assessments prior to the launch or use of such products, practices and technologies; and

(b) take appropriate measures to manage and mitigate the risks.

20. (1) A relevant person shall ensure that all cross border wire transfers are always accompanied by —

(a) required and accurate originator information, which includes —

- (i) the name of the originator;
 - (ii) the originator account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction; and
 - (iii) the originator's address, or national identity number, or customer identification number, or date and place of birth;
- (b) the following required beneficiary information —
- (i) the name of the beneficiary; and
 - (ii) the beneficiary account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

(2) Where several individual cross border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries —

- (a) the batch file shall contain required and accurate originator information as set out in paragraph (1)(a), and full beneficiary information, that is fully traceable within the beneficiary country; and
- (b) the relevant person shall include the originator's account number or unique transaction reference number.

(3) For domestic wire transfers, the ordering relevant person shall ensure that the information accompanying the wire transfer shall include originator information as specified in paragraph (1).

(4) The ordering relevant person shall maintain all originator and beneficiary information collected, in accordance with section 17F of the Act and regulation 14.

(5) The ordering relevant person shall not execute the wire transfer where it does not comply with the requirements specified in paragraphs (1) to (4).

(6) For cross border wire transfers, an intermediary financial institution shall ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it.

(7) Where technical limitations prevent the required originator or beneficiary information accompanying a cross border wire transfer from remaining with a related domestic wire transfer, the intermediary financial institution shall keep a record, for at least 7 years, of all the information received from the ordering financial institution or another intermediary financial institution.

(8) Intermediary financial institutions shall take reasonable measures, which are consistent with straight-through processing, to identify cross border wire transfers that lack required originator information or required beneficiary information.

(9) Intermediary financial institutions shall have risk-based policies and procedures for determining —

(a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and

(b) the appropriate follow-up action.

(10) Beneficiary financial institutions shall take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify cross border wire transfers that lack required originator information or required beneficiary information.

(11) A beneficiary financial institution shall verify the identity of the beneficiary, where the

identity has not been previously verified, and maintain this information in accordance with section 1 7F of the Act and regulation 14.

(12) A beneficiary financial institution shall have risk-based policies and procedures for determining —

- (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and
- (b) the appropriate follow-up action.

(13) MVTs providers shall comply with all of the relevant requirements of this regulation in the countries in which they operate, directly or through their agents.

(14) A MVTs provider that controls both the ordering and the beneficiary side of a wire transfer shall —

- (a) take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and
- (b) file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the FIU.

(15) This regulation shall not cover the following types of payments —

- (a) any transfer that flows from a transaction carried out using a credit or debit or prepaid card for the purchase

of goods or services, so long as the credit or debit or prepaid card number accompanies all transfers flowing from the transaction provided that, when a credit or debit or prepaid card is used as a payment system to effect a person-to-person wire transfer, the transaction shall be governed by this regulation, and the necessary information should be included in the message; and

(b) bank-to-bank transfers and settlements, where both the originator person and the beneficiary person are financial institutions acting on their own behalf

(16) In this regulation —

“intermediary financial institution” means a relevant person in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution;

“ordering financial institution” means the relevant person who initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator;

“relevant person” means a bank or foreign exchange dealer;

“straight-through processing” means payment transactions that are conducted electronically without the need for manual intervention.

Amended by [\[Act No. 9 of 2019\]](#)

21. (1) Subject to this regulation, a reporting person may rely on a third party to introduce business or to perform the CDD measures under regulation 3(1)(a), (c) and (d):

(2) Where a reporting person relies on a third party to introduce business or perform the CDD measures set out under paragraph (1), he shall —

(a) obtain immediately the necessary information required under regulation 3(1)(a), (c) and (d);

(b) take steps to satisfy himself that copies of identification data and other relevant documentation related to CDD requirements shall be made available from the third party upon request without delay;

- (e) satisfy himself that the third party is regulated and supervised or monitored for the purposes of combating money laundering and terrorism financing, and has measures in place for compliance with CDD and record keeping requirements in line with the Act and these regulations.

(3) A reporting person shall not rely on a third party based in a high risk country referred to in regulation 24.

(4) Where a reporting person relies on a third party that is part of the same financial group, the host or home supervisors may consider that the requirements of paragraphs (1), (2) and (3) are met, where —

- (a) the group applies CDD and record-keeping requirements and programmes against money laundering and terrorism financing, in accordance with the Act and these regulations;
- (b) the implementation of those CDD and record-keeping requirements and programmes against money laundering and terrorism financing is supervised at a group level by a competent authority; and
- (c) any higher country risk is adequately mitigated by the group's policies to combat money laundering and terrorism financing.

Amended by [\[GN No. 122 of 2018\]](#); [\[Act No. 9 of 2018\]](#)

22. (1) Every reporting person shall implement programmes against money laundering and terrorism financing having regard to the money laundering and terrorism financing risks identified and the size of its business, which at a minimum shall include the following internal policies, procedures and controls —

- (a) designation of a compliance officer at senior management level to be responsible for the implementation and ongoing compliance of the reporting person with

internal programmes, controls and procedures with the requirements of the Act and these regulations;

- (b) screening procedures to ensure high standards when hiring employees;
- (c) an ongoing training programme for its directors, officers and employees to maintain awareness of the laws and regulations relating to money laundering and terrorism financing to —
 - (i) assist them in recognising transactions and actions that may be linked to money laundering or terrorism financing; and
 - (ii) instruct them in the procedures to be followed where any links have been identified under sub subparagraph (i); and
- (d) an independent audit function to review and verify compliance with and effectiveness of the measures taken in accordance with the Act and these regulations.

(2) For the purpose of paragraph (1), the compliance officer shall have unrestricted access upon request to all books, records and employees of the reporting person as necessary for the performance of his functions.

(3) The functions of the compliance officer designated under paragraph (1) shall include

—

- (a) ensuring continued compliance with the requirements of the Act and regulations subject to the ongoing oversight of the board of the reporting person and senior management;
- (b) undertaking day-to-day oversight of the program for combating money laundering and terrorism financing;

- (c) regular reporting, including reporting of noncompliance, to the board and senior management; and
- (d) contributing to designing, implementing and maintaining internal compliance manuals, policies, procedures and systems for combating money laundering and terrorism financing.

23. (1) Every reporting person operating in a group structure shall implement group-wide programme against money laundering and terrorism financing, which shall be applicable, and appropriate to, all branches and subsidiaries of the group and which shall include —

- (a) the internal policies, procedures and controls set out in regulation 22;
- (b) policies and procedures for sharing information required for the purposes of customer due diligence and money laundering and terrorism financing risk management;
- (c) procedures to ensure that group-level compliance, audit, Money Laundering and Reporting Officer shall have the power to request customer, account and transaction information from branches and subsidiaries as necessary to perform their functions in order to combat money laundering and terrorism financing;
- (d) the provision by the group-level functions to branches and subsidiaries, of information and analysis of transactions or activities which appear unusual when relevant and appropriate to risk management; and
- (e) adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

(2) A reporting person shall ensure that its foreign branches and subsidiaries —

- (a) apply measures to combat money laundering and terrorism financing consistent

with the home country requirements, where the minimum requirements of the host country are less strict than those of the home country, to the extent that host country laws and regulations permit; and

- (b) where the host country does not permit the proper implementation of anti-money laundering and combating the financing of terrorism measures, apply appropriate additional measures to manage the money laundering and terrorism financing risks, and inform their home supervisors.

24. (1) For the purposes of these regulations and section 17C (3) and 17H of the Act, in identifying a high risk country, due consideration shall be given to —

- (a) strategic deficiencies in the anti-money laundering and combating the financing of terrorism legal and institutional framework, in particular in relation to —
 - (i) criminalisation of money laundering and terrorism financing;
 - (ii) measures relating to CDD;
 - (iii) requirements relating to record-keeping;
 - (iv) requirements to report suspicious transactions;
 - (v) the availability of accurate and timely information of the beneficial ownership of legal persons and arrangements to competent authorities;
- (b) the powers and procedures of the country's competent authorities for the purposes of combating money laundering and terrorist financing including appropriately effective, proportionate and dissuasive sanctions, as well as the country's practice in cooperation and exchange of information with overseas competent authorities;
- (c) the effectiveness of the country's system for combating money laundering and

terrorism financing in addressing money laundering or terrorist financing risks.

(2) For the purpose of paragraph (1), relevant evaluations, assessments or reports drawn up by international organisations and

standard setters with competence in the field of preventing money laundering and combating terrorist financing shall be taken into account.

(3) A reporting person shall apply enhanced due diligence, proportionate to the risks, to business relationships and transactions with natural and legal persons from countries for which this is called for by the Financial Action Task Force.

Amended by [\[GN No. 122 of 2018\]](#); [\[Act No. 9 of 2019\]](#)

25. (1) A reporting person shall examine, as far as reasonably possible, the background and purpose of all transactions that —

- (a) are complex transactions;
- (b) are unusually large transactions;
- (c) are conducted in an unusual pattern; or
- (d) do not have an apparent economic or lawful purpose.

(2) Where the risks of money laundering or terrorism financing are higher, a reporting person shall conduct enhanced CDD measures consistent with the risk identified.

26. (1) A reporting person shall appoint a Money Laundering Reporting Officer to whom an internal report shall be made of any information or other matter which comes to the attention of any person handling a transaction and which, in the opinion of the person gives rise to knowledge or reasonable suspicion that another person is engaged in money laundering or the financing of terrorism.

(2) A reporting person shall appoint a Deputy Money Laundering Reporting Officer to perform the duties of the Money Laundering Reporting Officer in his absence.

(3) Where the reporting person is a member of a relevant profession or occupation under the Act, and due to the nature and size of its business or activity is unable to appoint a Money Laundering Reporting Officer and a Deputy Money Laundering Reporting Officer, he shall establish, maintain and operate reporting and disclosure procedures in accordance with the Act, and as may be specified by a relevant regulatory body.

(4) The Money Laundering Reporting Officer and the Deputy Money Laundering Officer shall —

- (a) be sufficiently senior in the organisation of the reporting person or have sufficient experience and authority; and
- (b) have a right of direct access to the board of directors of the reporting person and have sufficient time and resources to effectively discharge his functions.

27. Subject to regulation 26(3), a reporting person shall establish, document, maintain and operate reporting procedures that shall —

- (a) enable all its directors or, as the case may be, partners, all other persons involved in its management, and all appropriate employees to know to whom they should report any knowledge or suspicion of money laundering and terrorism financing activity;
- (b) ensure that there is a clear reporting chain under which that knowledge or suspicion will be passed to the Money Laundering Reporting Officer;
- (c) require reports of internal disclosures to be made to the Money Laundering Reporting Officer of any information

or other matters that come to the attention of the person handling that business and

which in that person's opinion gives rise to any knowledge or suspicion that another person is engaged in money laundering and terrorism financing activity;

- (d) require the Money Laundering Reporting Officer to consider any report in the light of all other relevant information available to him for the purpose of determining whether or not it gives rise to any knowledge or suspicion of money laundering or terrorism financing activity;
- (e) ensure that the Money Laundering Reporting Officer has full access to any other information that may be of assistance and that is available to the reporting person; and
- (f) enable the information or other matters contained in a report to be provided as soon as is practicable to the FLU where the Money Laundering Reporting Officer knows or suspects that another person is engaged in money laundering or terrorism financing activities.

28. (1) Where a reporting person identifies any suspicious activity in the course of a business relationship or occasional transaction the reporting person shall —

- (a) consider obtaining enhanced CDD in accordance with regulation 12; and
- (b) make an internal disclosure in accordance with the procedures established under regulation 27.

(2) Where a reporting person identifies any unusual activity in the course of a business relationship or occasional transaction the reporting person shall —

- (a) perform appropriate scrutiny of the activity;
- (b) obtain enhanced CDD in accordance with regulation 12; and
- (c) consider whether to make an internal disclosure in accordance with the reporting

procedures established under regulation 27.

29. (1) Subject to regulation 26(3), where an internal disclosure has been made, the Money Laundering Reporting Officer shall assess the information contained within the disclosure to determine whether there are reasonable grounds for knowing or suspecting that the activity is related to money laundering, terrorism financing or proliferation financing.

(2) The Money Laundering Reporting Officer shall forthwith make a report in accordance with section 14 of the Act to the FIU where he knows or has reason to believe that an internal disclosure may be suspicious.

(3) Where FIU receives a report made by a Money Laundering Reporting Officer pursuant to paragraph (2), it shall acknowledge receipt of the report forthwith.

Amended by [\[Act No. 9 of 2019\]](#)

30. (1) A reporting person must establish and maintain separate registers of—

(a) all internal disclosures; and

(b) all external disclosures.

(2) The registers of internal disclosures and external disclosures may be contained in a single document if the details required to be included in those registers under paragraph (3) can be presented separately for internal disclosures and external disclosures upon request by a competent authority.

(3) The registers must include details of—

(a) the date on which the report is made;

(b) the person who makes the report;

(c) for internal disclosures, whether it is made to the Money Laundering Reporting

Officer or Deputy Money Laundering Reporting Officer; and

(d) information sufficient to identify the relevant papers.

31. A reporting person shall establish and maintain appropriate procedures for monitoring and testing compliance with the Anti-Money Laundering or Combatting the Financing of Terrorism requirements, having regard to ensuring that —

(a) the reporting person has robust and documented arrangements for managing the risks identified by the business risk assessment conducted in accordance with section 17 of the Act for compliance with those requirements;

(b) the operational performance of those arrangements is suitably monitored; and

(c) prompt action is taken to remedy any deficiencies in arrangements.

32. Deleted by [\[Act No. 9 of 2019\]](#)

33. Any person who contravenes these regulations shall commit an offence and shall on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

34. The Financial Intelligence and Anti-Money Laundering Regulations 2003 are revoked.

35. These regulations shall come into operation on 1 October 2018.

Made by the Minister on 28 September 2018.