ශ්‍රී ලංකා ප්‍රජාතාන්ත්‍රික සමාජවාදී ජනරජයේ ගැසට් පත්‍රය

අති විශෙෂ

The Gazette of the Democratic Socialist Republic of Sri Lanka

EXTRAORDINARY

අංක 2511/55 - 2026 ඔක්තෝබර් මස 22 වැනි බ්‍රහස්පතින්දා - 2026.10.22

No. 2511/55 - THURSDAY, OCTOBER 22, 2026

(Published by Authority)

PART I : SECTION (I) — GENERAL

Government Notifications

L. D.-B 3/2006 (II)

FINANCIAL TRANSACTIONS REPORTING ACT, No. 6 OF 2006

RULES made by the Head of the Financial Intelligence Unit under section 29A read with section 2 and section 5 of the Financial Transactions Reporting Act, No. 6 of 2006.

Head of the Financial Intelligence Unit

Colombo,
22nd October 2026.

Rules

1. These rules may be cited as the Designated Non-Finance Businesses or Professions (Customer Due Diligence) Rules, No. 2 of 2026.

2. These rules shall apply to the following Designated Non-Finance Businesses or Professions (hereinafter referred to as the "DNFBP"):-

(a) any person engaging in or carrying out any casino within the meaning of gambling under the Gambling Regulatory Authority Act, No. 17 of 2025;

1A- G 48398 - 23 (10/2026)

This Gazette Extraordinary can be downloaded from www.documents.gov.lk

(b) real estate agents including property developers;

(c) dealers in precious metals and dealers in precious and semi-precious stones, including but not limited to, metals and stones covered by the National Gem and Jewellery Authority Act, No. 50 of 1993;

(d) lawyers, notaries, other independent legal professionals or accountants when they prepare for or carry out transactions for their clients in relation to any one or more of the following activities :-

(i) buying and selling of real estate;

(ii) managing of client money, securities or other assets;

(iii) management of bank, savings or securities accounts;

(iv) organization of contributions for the creation, operation or management of companies;

(v) creation, operation or management of legal persons or legal arrangements or the buying and selling of business entities.

(e) trust or company service providers not otherwise covered by paragraphs (i) to (v) of paragraph (d), which as a business, provide any one or more of the following services to third parties:-

(i) formation or management of legal persons or legal arrangements;

(ii) acting as or arranging for another person to act as, a director or secretary of a company, a partner of a partnership or a similar position in relation to other legal persons;

(iii) providing a registered office, business address or accommodation, correspondence or administrative address for a company, partnership or any other legal person or legal arrangement;

(iv) acting as a trustee or arranging for another person to act as a trustee of an express trust, or performing the equivalent function for any other form of legal arrangement; or

(v) acting as, or arranging for another person to act as, a nominee shareholder for another person.

(f) any offshore unit of any business, profession or activity referred to in paragraphs (a) to (e), or (g) in accordance with the definition provided for such offshore unit in any other written law; and

(g) any person engaged in any businesses specified in paragraphs (a) to (f) which shall be registered or licensed under the Colombo Port City Economic Commission Act, No. 11 of 2021.

PART I

MONEY LAUNDERING, TERRORIST FINANCING AND FINANCING OF PROLIFERATION OF WEAPONS OF MASS DESTRUCTION RISK MANAGEMENT

3. Every DNFBP shall take measures specified in these rules for the purpose of identifying, assessing and understanding its money laundering, terrorist financing and financing of proliferation of weapons of mass destruction risks (hereinafter referred to as the “risk”) associated with its customers, the countries or regions in which those customers are engaged in business, its products, services, transactions and delivery channels by conducting customer due diligence (hereinafter referred to as the "CDD") and apply a risk-based approach for allocating resources, monitoring, managing and mitigating such risk.

4. The intensity and extensiveness of risk management shall be commensurate with the level of risk and be proportionate to the nature, scale and complexity of the DNFBP's activities and its risk profile by applying a risk-based approach.

5. (1) Every DNFBP shall conduct appropriate processes, including the following, in identifying, assessing and understanding its risk:-

(a) carry out institutional risk assessment to determine the level of risk and the appropriate types of mitigation to be applied in relation to the level of risk by considering all relevant risk factors including but not limited to the national risk assessment on money laundering, terrorist financing and financing of proliferation of weapons of mass destruction;

(b) document such risk assessment including findings and action plans, to manage the risk, with timelines;

(c) keep the risk assessment up-to-date through a review, at least annually and more frequently as needed;

(d) advise the Board of Directors or senior management of the DNFBP of such risk assessment and the measures to manage the risk;

(e) obtain the approval of the Board of Directors or senior management of the DNFBP for such risk assessment and any update thereto; and

(f) provide risk assessment information to the relevant supervisory authority, self-regulatory body, competent authority or the Financial Intelligence Unit as the case may be.

(2) It shall be the duty of the Board of Directors or senior management of the DNFBP to provide sufficient resources required to conduct the processes specified in sub rule (1).

6. A DNFBP's risk management shall be affiliated and integrated with the overall enterprise-wide risk management of the DNFBP.

7. Every DNFBP shall have risk control and mitigation measures including the following :-

(a) internal policies, controls, procedures and systems approved in the manner specified in rule 12;

(b) programme to monitor, review and test the implementation of those policies, controls, procedures and systems, at least annually, to ensure they remain fit for purpose;

(c) training and awareness programmes for employees and the Board of Directors or senior management of the DNFBP as specified in rule 14(e); and

(d) timely reporting to the Board of Directors or senior management of the DNFBP as specified in rule 8.

8. (1) Every DNFBP shall provide a timely report of the effectiveness of the risk controls and mitigation measures based on the findings of its risk assessment and regular review mechanisms to its Board of Directors or senior management. The frequency of reporting shall be commensurate with the level of risk involved, the operating environment and overall sectoral risk.

(2) The report referred to in sub rule (1) shall include the following:-

(a) the results of monitoring activities carried out by the DNFBP for combating the risk (such as the level of the DNFBP's exposure to risk, break-down of risk exposures based on customers, products, geographical locations of operations, delivery channels and transactions, trends of suspicious transaction reports and threshold reports, judicial pronouncements and freezing actions under any regulation made in terms of the United Nations Act, giving effect to the United Nations Security Council Resolutions on targeted financial sanctions related to prevention and suppression of terrorism and terrorist financing and prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing or in terms of any other regulation made under the United Nations Act giving effect to any other related United Nations Security Council Resolution);

(b) the outcome of risk assessments conducted prior to the launch or use of new products, services, practices, delivery mechanisms, and technologies;

(c) details of recent risk typologies identified either internally or externally, the modus operandi and its impact or potential impact on the DNFBP;

(d) recent developments in written laws on anti-money laundering, countering the financing of terrorism and financing of proliferation of weapons of mass destruction and its implications for the DNFBP; and

(e) the extent to which the institutional risk assessment reflects the findings of the national risk assessment.

9. (1) Every DNFBP shall conduct risk profiling of its customers, considering the following: -

(a) the category of customers such as resident or non-resident, occasional or one-off, legal persons, legal arrangements, non-governmental organizations, not-for-profit organizations, politically exposed persons, or customers engaged in different types of occupations;

(b) the countries and regions in which such customers are engaged in business;

(c) the products,services, transactions and delivery channels used by the customer such as cash-based, face-to-face or non-face-to-face or cross-border, digital banking; and

(d) any other information regarding the customer.

(2) Notwithstanding the provisions of sub rule (1) a DNFBP may conduct risk profiling of occasional customers under these rules if the need arises.

(3) Every DNFBP may use the information obtained under sub rule (1) of rule 22 for the purpose of considering the matters specified in sub rule (1) of this rule for initial risk profiling.

10. The risk control and mitigation measures implemented by every DNFBP in relation to its customers shall be commensurate with the customer’s risk profile conducted under rule 9.

11. Every DNFBP shall-

(a) prior to establishing a business or professional relationship with a customer, comply with the provisions of rule 22; and

(b) upon the initial acceptance of a customer, periodically conduct due diligence review in accordance with rule 34 and update the customer's risk profile based on the current level of risk of such customer.

Internal Controls, Policies, Procedures, Compliance, Audit and Training

12. (1) Every DNFBP shall formulate an internal policy approved by its Board of Directors or senior management subject to the written laws in force for the time being, on anti-money laundering, countering the financing of terrorism and financing of proliferation of weapons of mass destruction. Such policy shall be reviewed annually or sooner by the DNFBP, whenever there are changes to the risk or such written laws, and the approval for such reviewed policy shall be obtained from its Board of Directors or senior management.

(2) The detailed procedures, controls and systems shall be developed by each DNFBP in compliance with such policy and be approved by the Board of Directors or senior management.

(3) Such policy, procedures, controls and systems shall include but not limited to, risk assessment procedures, CDD measures, requirement of record retention, handling of attempted transactions, reliance on third parties, compliance with targeted financial sanctions, anti-money laundering, countering the financing of terrorism and financing of proliferation of weapons of mass destruction audits, the detection and internal reporting procedure of unusual or suspicious transactions, the obligation to report suspicious transactions in terms of section 7 and transactions specified under section 6 of the Act to the Financial Intelligence Unit, transaction monitoring, handling of breaches, escalation mechanism, whistleblowing, testing, new product, service, delivery channel or technology approvals, avoidance of tipping-off and confidentially obligations and termination of business or professional relationship.

13.Every DNFBP shall in formulating policies, procedures, systems, and controls take into consideration the risk that may arise from the use of new or developing technologies, including those having features of anonymity and inconsistency with the CDD measures specified in Part II of these rules.

14.Every DNFBP shall -

(a) appoint a compliance officer in terms of the provisions of the Act, and inform forthwith the Financial Intelligence Unit on the appointment and any changes to the appointment of such compliance officer;

(b) provide the compliance officer with sufficient resources to ensure the duties, functions and obligations of the DNFBP under the Act and these rules are performed and discharged;

(c) ensure that such compliance officer or any other person authorized to assist the compliance officer or act on behalf of the compliance officer, has prompt access to all customer records and other relevant information, systems and personnel which may be required to discharge the compliance officer’s functions;

(d) develop and implement a comprehensive employee and agent due diligence and screening procedure to be carried out at the time of appointing, entering into a contract or any agreement or hiring of employees whether permanent, contractual or outsourced or agents;

(e) design and implement, on-going, periodic training and awareness programmes for employees including the Board of Directors or senior management of the DNFBP, in order to effectively implement the regulatory requirements and internal policies and procedures relating to risk management. The training and awareness programmes shall include, but not limited to, understanding the relevant written laws, institutional overall risk, new developments in money laundering, terrorist financing and financing of proliferation of weapons of mass destruction

techniques, methods and trends and their responsibilities relating to the combating of the risk, requirements relating to CDD, targeted financial sanctions and identifying suspicious or unusual transactions and reporting obligations including suspicious transactions; and

(f) maintain an independent audit function that is adequately resourced and able to regularly assess the effectiveness of the DNFBP's implementation of internal policies, procedures controls and systems and, its compliance with the Act, rules, regulations, directions, circulars and guidelines made or issued under the Act.

Branches, Majority-owned Subsidiaries and Group of companies

15. Every group of companies consisting of any DNFBP and any other entity shall, subject to the provisions of the Act and these rules, implement group-wide programmes which shall be applicable and appropriate for all branches and majority-owned subsidiaries of the group with a view to combatting money laundering, terrorist financing and financing of proliferation of weapons of mass destruction and shall include the following in addition to the measures referred to in rule 14:-

(a) formulate policies, procedures, controls and systems for sharing information within the group of companies consisting of any DNFBP and any other entity for purposes of conducting CDD and risk management;

(b) provide or receive information of customers, accounts, transactions, analysis of unusual transactions and underlying information of such transactions, typologies and of audits, to or from all branches and majority-owned subsidiaries of the group when necessary for implementing the anti-money laundering, countering the financing of terrorism and financing of proliferation of weapons of mass destruction measures;

(c) maintain adequate safeguards on the confidentiality and use of information exchanged within the group including safeguards in relation to divulging of information; and

(d) ensure effective implementation of its anti-money laundering, countering the financing of terrorism and financing of proliferation of weapons of mass destruction framework in branches and majority-owned subsidiaries and group of companies consisting of any DNFBP and any other entity.

16. (1) Every DNFBP shall ensure that its foreign branches and majority-owned subsidiaries and group of companies consisting of any DNFBP and any other entity apply measures which are consistent with the Act, regulations, rules, Orders and directions made or issued under the Act to combat money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, where the relevant written laws of the relevant foreign country provide less stringent requirements than those provided by the Act, regulations, rules, Orders and directions made or issued under the Act.

(2) Where the relevant written laws of a foreign country do not permit the implementation of anti-money laundering, countering the financing of terrorism and financing of proliferation of weapons of mass destruction measures which are consistent with the Act, regulations, rules, Orders and directions made or issued under the Act, then the DNFBP shall apply appropriate additional measures to manage and mitigate the risk and inform the Financial Intelligence Unit and the relevant supervisory authority of the measures that have not been implemented, risk stemming therefrom and the additional measures implemented to address the risk.

(3) For the purpose of paragraph (2), 'additional measures' shall include extra precautionary measures and increased oversight and controls.

New Technologies (Products, Services and Business or Professional Practices)

17. (1) Every DNFBP shall identify, assess, understand, manage, monitor and mitigate the risk that may arise in relation to the development of new products, services and business or professional practices, including new delivery mechanisms and the use of new or developing technologies for both new and existing products and services.

(2) Every DNFBP shall-

(a) undertake a risk assessment prior to the launch or use of such new products, services, business or professional practices, delivery mechanisms, and technologies; and

(b) take appropriate measures to manage and mitigate the risk which may arise in relation to the development and use of such new products, services, business or professional practices, delivery mechanisms, or technologies as the case may be.

PART II

CUSTOMER DUE DILIGENCE (CDD)

18. (1) In terms of the provisions of subsection (3) section 2 of the Act, a DNFBP shall not open, operate or maintain an account, where the holder of such account cannot be identified, including any anonymous account or any account identified by number only, any account or any business or professional relationship which to the knowledge of the DNFBP is being operated under a fictitious or false name (hereinafter referred to as "Fictitious or Anonymous Account").

(2) A Fictitious or Anonymous Account includes an account where the ownership is transferrable without the knowledge of the DNFBP and accounts that are operated and maintained with the account holder's name omitted.

19. Every DNFBP shall maintain information in such a manner that the records and information in relation to a given customer of such DNFBP can be readily retrievable.

20. A DNFBP shall not maintain information of transaction or professional relationship separate from the DNFBP's standard operational processes, controls, systems or procedures.

21. A DNFBP shall conduct CDD measures specified in these rules, in the following instances:-

(a) in the case of DNFBPs referred to in paragraph (a) of rule 2, in relation to a customer engaging in financial transactions in Sri Lanka Rupees or in any foreign currency equivalent to or above United States Dollars three thousand (3,000);

(b) in the case of DNFBPs referred to in paragraph (b) of rule 2, when such a DNFBP is involved in transactions for a client concerning the buying and selling of real estate and with respect to both the purchasers and vendors of the real estate;

(c) in the case of DNFBPs referred to in paragraph (c) of rule 2, when such a DNFBP engages any cash transaction with a customer in Sri Lanka Rupees or in any foreign currency equivalent to or above United States Dollars fifteen thousand (15,000);

(d) in the case of DNFBPs referred to in paragraph (d) of rule 2, when they prepare for or carry out transactions for their clients in relation to any one or more of the activities specified in items (i) to (v) in paragraph (d) of rule 2;

(e) in the case of DNFBPs referred to in paragraph (e) of rule 2, when providing any one or more of the services specified in items (i) to (v) in paragraphs (e) of rule 2 to third parties;

(f) in the case of DNFBPs referred to in paragraphs (b), (d) and (e) of rule 2, when any customer conducts occasional transactions involving an amount exceeding Sri Lanka Rupees two hundred thousand (200,000) or its equivalent in any foreign currency where the transaction is carried out in a single operation or in multiple operations that appear to be linked or when such DNFBPs establish a business or professional relationship with any customer;

(g) in the case of DNFBPs referred to in paragraphs (f) and (g) of rule 2, in the instances specified in paragraphs (a) to (f) of this rule;

(h) where any DNFBP has any suspicion or has reasonable grounds to believe that any customer is involved in money laundering or terrorist financing activities or financing of proliferation of weapons of mass destruction or any unlawful activity, regardless of the amount; or

(i) where the DNFBP has any doubt about the veracity or adequacy of customer identification documents or information already obtained.

22. (1) Every DNFBP in conducting CDD measures under these rules shall obtain up-to date and accurate information specified in Schedule hereto and shall-

(a) identify the customer, whether permanent or occasional, whether a natural person, legal person or legal arrangement and verify such customer's identity on the basis of any official document or other reliable source document, data or information;

(b) where a beneficial owner exists, identify such beneficial owner and take reasonable measures to verify the identity of that beneficial owner using any official document, relevant information or data obtained from a reliable source, so as to satisfy itself as to the identity of such beneficial owner;

(c) understand and, as appropriate, obtain information using any other relevant document, material or data on the purpose and intended nature of the business or professional relationship with a customer and of each account;

(d) where one or more natural persons are acting on behalf of a customer, identify the natural persons who act on behalf of the customer and verify the identity and authority of such persons to act on the basis of official documents or other reliable source documents, information or data such as letters of authorization, board resolutions, powers of attorney or letters of administration or letters of probate;

(e) record the information for the purpose of identifying and verifying customers and for the purpose of initial risk profiling as specified in rule 9;

(f) conduct ongoing due diligence throughout the course of the business or professional relationship; and

(g) conduct ongoing transaction monitoring of all transactions and scrutinize any transactions executed on behalf of the customer throughout the course of the business or professional relationship.

(2) The DNFBPs referred to in paragraph (a) of rule 2 may conduct measures to identify customers at the point of entry to a casino and shall link the CDD information of a particular customer to the transactions executed by such customer in the casino.

23. Where any DNFBP is unable to comply with CDD measures specified in these rules, such DNFBP shall –

(a) in relation to a new customer, not commence the business or professional relationship or perform the transaction; or

(b) in relation to a customer who has already established a business or professional relationship, terminate such business or professional relationship,

and consider making a suspicious transaction report in relation to such customer.

24. Where any DNFBP suspects or has reasonable grounds to suspect the commission of an offence of money laundering, terrorist financing or financing of proliferation of weapons of mass destruction or any unlawful activity and if there are reasons to believe that conducting CDD measures will tip off the customer, such DNFBP is permitted not to conduct CDD measures and shall immediately make a suspicious transaction report.

Risk Based Due Diligence

25. (1) Without prejudice to the provisions of rule 22, where any customer is rated as a customer posing a low risk, a DNFBP may conduct, but not limited to, the following simplified CDD measures as such DNFBP may deem appropriate-

(a) verifying the identity of the customer and the beneficial owner after the establishment of the business or professional relationship (delayed verification);

(b) reducing the frequency of periodic reviews of customer relationship;

(c) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business or professional relationship, but inferring the purpose and nature from the type of transactions or business or professional relationship established.

(2) The simplified measures conducted under sub rule (1) shall only be in relation to establishing a business or professional relationship and conducting a periodic review of the business or professional relationship.

26. (1) Where any customer is rated as a customer posing a high risk, a DNFBP shall conduct the following enhanced CDD measures for such customer, in addition to the CDD measures specified in rule 22 and any other measures as such DNFBP may deem necessary:-

(a) obtain and verify the following as applicable -

(i) additional information on customer, occupation, volume of assets, updated residential address and any other appropriate information;

(ii) credible open source information including information available in public databases;

(iii) more regularly updating the identification information of the customer and beneficial owner of the customer;

(iv) additional details on the intended nature and purpose of the business or professional relationship;

(v) additional information on the source of funds or source of wealth of the customer;

(vi) information on the reasons for intended or performed transactions; and

(vii) any other information the DNFBP may deem necessary; and

(b) the following approvals and monitoring measures -

(i) approval of senior management to commence or continue the business or professional relationship;

(ii) enhanced monitoring of the business or professional relationship, including selection and review of transaction patterns requiring further examination;

(iii) periodic review of customer relationship within one year.

(2) Such DNFBP shall, in conducting the enhanced CDD measures, determine the appropriate measures applicable to each and every customer.

Delayed Verification

27. Every DNFBP shall verify the identity of the customer and the beneficialowner prior to or during the course of establishing a business or professional relationship or conducting a transaction for an occasional customer:

Provided however, where the level of risk of the customer is assessed as low and the verification is not possible at the time of establishing the business or professional relationship, the DNFBP shall subsequently complete the verification (hereinafter referred to as the "delayed verification"):

Provided further, where delayed verification is allowed-

(a) the verification shall be completed as soon as reasonably practicable but not later than fourteen working days from the date of establishing the business or professional relationship;

(b) the delay shall be essential so as not to interrupt the DNFBP's normal conduct of business;

(c) there shall be no suspicion or reasonable grounds to believe the existence of the risk, and the additional risks occurring from such delayed verification shall be low;

(d) there shall be an internal policy and procedure that address delayed verification including but not limited to the circumstances it may be permitted, mitigating and risk management mechanisms, and internal reporting; and

(e) there shall be no reasonable grounds to believe that customer and beneficial owner, where applicable, verification may not be possible within the fourteen working days.

28. Every DNFBP shall take measures to mitigate the risk of delayed verification, including recording the conditions under which the customer may utilise the business or professional relationship prior to verification, which may include limiting the number, type and value of transactions that can be performed, and monitoring large and complex transactions not aligned with expected customer behaviour.

29. A DNFBP shall not, under any circumstances, establish a business or professional relationship or conduct any transaction with a customer prior to verifying the identity of such customer and beneficial owner, if any, where the risk level of such customer is assessed as high.

Customer and Transaction Monitoring

30. Every DNFBP shall monitor all business or professional relationships on an ongoing basis to ensure that the transactions are consistent with the information obtained under these rules, the risk profile of such customer and the DNFBP's knowledge of such customer.

31. (1) Every DNFBP shall obtain information and examine the background and purpose of all complex, unusually large transactions and all unusual patterns of transactions, which have no apparent economic or prima facie lawful purpose.

(2) The background and purpose of such transactions shall be inquired into and findings shall be kept on record with a view to making such information available to the relevant competent authority, supervisory authority or the Financial Intelligence Unit when required to do so.

32. Every DNFBP shall increase the controls and select patterns of transactions that need further examination, in relation to high risk business or professional relationships and identify any suspicion, if available.

33. Every DNFBP shall have an effective internal mechanism to report any suspicious transaction to the DNFBP's compliance officer for appropriate action, in compliance with the Act and these rules.

34. (1) Every DNFBP shall periodically–

(a) review all customer relationships. Such reviews shall include assessing the adequacy, accuracy and up-to-dateness of customer information held by the DNFBP, changes in customer profile such as beneficial ownership, customer behaviour, delivery channels, products used, source of funds, client's account activity and verification of customers against any regulation made in terms of the United Nations Act, identification of politically exposed persons and;

(b) re-assess and re-classify the customer's risk rating, as needed.

(2) The review period and procedures thereof shall be decided by each DNFBP on a risk-based approach as laid down in its internal policy for anti-money laundering, countering the financing of terrorism and financing of proliferation of weapons of mass destruction:

Provided however, for high risk customers a periodic review shall be conducted at least once during a period of one year.

(3) Every DNFBP shall ensure that periodic reviews are completed on or before the next periodic review cycle date.

(4) Every DNFBP shall-

(a) carry out event-driven reviews, separate from and in addition to periodic reviews. An event-driven review shall be conducted within a reasonable period of such event; and

(b) revise the periodic review cycle of the customer based on the outcome of the event-driven review.

Existing Customers

35. Every DNFBP shall conduct CDD measures as may be appropriate on its existing customers having regard to its own assessment of materiality and the risk but without compromising the identity and verification requirements. In assessing the materiality and risk of an existing customer, a DNFBP may consider the following:-

(a) the nature and circumstances surrounding the transaction including the significance of the transaction;

(b) any material change in the way the account or business or professional relationship is operated; or

(c) the insufficiency of information held on the customer or change in customer's information.

36. Every DNFBP shall conduct CDD measures on existing customer relationships at appropriate times, considering whether CDD measures have previously been conducted, the adequacy of documents, information, or data obtained, and ensuring that documents, information, or data collected through CDD measures are kept up-to-date and relevant through regular reviews of existing records.

Legal Persons and Legal Arrangements

37. Every DNFBP shall, in addition to the other provisions of these rules, in the case of a customer, who is not a natural person -

(a) understand the nature of the customer's business, its ownership and the control structure and take reasonable measures to determine the natural persons, who ultimately own or control the customer; and

(b) identify and verify the customer in terms of the requirements set out in Schedule hereto.

38. (1) In order to identify the beneficial owner in a legal person a DNFBP shall, at the minimum, obtain and take reasonable measures to verify the following :-

(a) the identity of the natural person, who ultimately has the controlling ownership interest in a legal person;

(b) the identity of all shareholders with equity interest of more than ten *per cent* with the requirement imposed on the legal person to inform of any change in the shareholders;

(c) if there is a doubt as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interest, the identity of the natural person, if any, exercising control of the legal person; and

(d) where no natural person is identified under the paragraphs (a), (b) or (c) the identity of the relevant natural person who holds the position of senior managing official of such legal person.

(2) Where a legal person's controlling ownership interest is vested with another legal person or legal arrangement, a DNFBP shall, identify and take reasonable measures to verify the natural person who controls such other legal person or legal arrangement.

39. In order to identify the beneficial owner in a legal arrangement, a DNFBP shall, at the minimum, obtain and take reasonable measures to verify the following:-

(a) in relation to trusts, including trusts created outside Sri Lanka but administered in Sri Lanka or with sufficient links to Sri Lanka, the identities of the author of the trust, the trustees, the beneficiary or class of beneficiaries and objects of a power and any other natural person exercising ultimate effective control over the trust including those who control through the chain of control or ownership;

(b) for other types of legal arrangements, other than trusts the identities of persons in equivalent or similar positions; and

(c) where the parties to a trust or other similar legal arrangement are legal persons or arrangements, beneficial owners of such legal person or arrangement.

Non-Governmental Organizations, Not-for-Profit Organizations or charitable institutions

40. Every DNFBP shall, in addition to the other provisions of these rules, conduct CDD measures when entering into a business or professional relationship with a Non-Governmental Organization (hereinafter referred to as "NGO"), a Not-for-Profit Organization (hereinafter, referred to as "NPO") or charitable institution to ensure that their accounts are used for and the transactions are commensurate with the declared objectives and purposes of such NGO, NPO or charitable institution as per their constituent documents.

41. The persons who are authorized to operate the accounts on behalf of any NGO, NPO or charitable institution and the members of the governing body of any NGO, NPO or charitable institution shall also be subject to CDD measures.

42. Every DNFBP shall review all existing relationships and monitor all transactions of a NGO, NPO or charitable institution to ensure that those organizations and institutions, their authorized signatories, members of their governing bodies and the beneficial owners are not linked with any designated person, group or entity as referred to in rule 52.

Business Relationships or Transactions where the customer is not physically present

43. (1) Every DNFBP may establish a non- face to face business or professional relationship or conduct a non- face to face transaction with a customer, only if such DNFBP has policies, procedures and controls in place to address any specific risk associated with such business or professional relationship or transaction.

(2) The policies, procedures and controls referred to in sub rule (1) shall include-

(a) appropriate measures to identify and verify the customer's identity that are equally effective as that for customers of face to face business or professional relationships and transactions;

(b) controls in order to avoid the risk posed in establishing and conducting business or professional relationships or transactions through information and communication technology;

(c) mechanisms for monitoring and reporting of potential risk that may be posed in establishing and conducting non face to face business or professional relationships or transactions.

Customers from high risk Countries or Jurisdictions

44. (1) Every DNFBP shall apply effective enhanced CDD measures that shall correspond to the risk to business or professional relationships and transactions with customers from high risk countries or jurisdictions.

(2) For the purposes of these rules, the "high risk countries or jurisdictions" mean-

(a) countries or jurisdictions identified by Financial Action Task Force as-

(i) subject to a call for action; or

(ii) under increased monitoring; and

(b) any country or jurisdiction specified by the Secretary to the Ministry of the Minister assigned the subject of Foreign Affairs, in consultation with the Secretary to the Ministry of the Minister assigned the subject of Defence, by Notification published in the *Gazette* as high risk countries or jurisdictions, independently, taking into account the existence of strategic deficiencies in anti-money laundering, countering the financing of terrorism and financing of proliferation of weapons of mass destruction and the lack of sufficient progress in addressing such deficiencies.

(3) The Head of the Financial Intelligence Unit shall publish the high risk countries or jurisdictions specified in sub rule (2), in its official website and shall advice weaknesses in anti-money laundering, countering the financing of terrorism and financing of proliferation of weapons of mass destruction systems of such countries.

45. Every DNFBP shall, in addition to enhanced CDD measures, apply appropriate counter measures, for high risk countries or jurisdictions referred to in sub rule (3) of rule 44, corresponding to the nature of the risk of such high risk countries or jurisdictions, as follows:-

(a) limiting business or professional relationship or financial transactions with high risk countries or jurisdictions or persons located in high risk countries or jurisdictions ;

(b) implementing stringent assessment and evaluation prior to opening of new branches or majority-owned subsidiaries of DNFBP in high risk countries or jurisdictions;

(c) reviewing, amending or terminating, if necessary, correspondent banking relationships with DNFBPs from high risk countries or jurisdictions;

(d) conducting enhanced external audits, by increasing the intensity and frequency of branches and majority-owned subsidiaries of the DNFBP or DNFBP group of companies located in high risk countries or jurisdictions; and

(e) applying enhanced transaction controls and conducting any other measures as may be specified by the Head of the Financial Intelligence Unit.

Politically Exposed Persons (PEPs)

46. (1) Every DNFBP shall, in addition to conducting CDD measures in relation to its customers, have risk management systems including policies, procedures and controls, to determine whether a customer or the beneficial owner of such customer, is or has been, a politically exposed person or is a family member or a close associate of a politically exposed person.

(2) Every DNFBP shall-

(a) obtain approval from the senior management of the DNFBP to enter into or continue the business or professional relationship where the customer or a beneficial owner of such customer, is or has been a politically exposed person or subsequently becomes a politically exposed person, or is a family member or a close associate of a politically exposed person;

(b) take reasonable measures to establish, by appropriate means, the sources of funds and wealth of a politically exposed person or a family member or a close associate of a politically exposed person; and

(c) conduct enhanced CDD and ongoing monitoring of the business or professional relationship where the customer or a beneficial owner of such customer, is a politically exposed person or subsequently becomes a politically exposed person, or is a family member or a close associate of a politically exposed person.

DNFBPs which rely on third parties

47. (1) A DNFBP may rely on a third party Financial Institution or DNFBPs to conduct CDD measures, including the identification of the customer and verification of such identification, identification and taking reasonable measures to verify the beneficial owner and understanding the nature and purpose of the business or professional relationship or to introduce business.

(2) The ultimate responsibility for such CDD measures conducted relying on a third party Financial Institution or DNFBP shall remain with the DNFBP relying on the third party Financial Institution or DNFBP, and such DNFBP shall-

(a) obtain immediately the necessary information relating to the CDD measures undertaken by the third party Financial Institution or DNFBP;

(b) take steps to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available by the third party Financial Institution or DNFBP without delay, upon request;

(c) satisfy itself that such third party Financial Institution or DNFBP is regulated, supervised or monitored for, and has measures to adhere to CDD and record-keeping requirements in compliance with the Act and these rules or any other applicable written law.

48. Every DNFBP which relies on a third party Financial Institution or DNFBP in another country shall, have regard to information available on the level of country risk, when determining the country of a third party Financial Institution or

DNFBP.

49. Where a DNFBP acting in accordance with rule 47 or 48 relies on a third party Financial Institution or DNFBP that forms part of the same DNFBP, financial group or group of companies, such DNFBP shall do so only where it ensures that -

(a) such group applies CDD measures and record-keeping requirements and implements anti-money laundering, countering the financing of terrorism and financing of proliferation of weapons of mass destruction programmes, in accordance with the Act and any rules, regulations, Orders and directions made or issued thereunder;

(b) the implementation of CDD measures and record-keeping requirements and anti-money laundering, countering the financing of terrorism and financing of proliferation of weapons of mass destruction programmes, is subject to supervision at group level by the Financial Intelligence Unit or any other relevant authority; and

(c) any risk arising from a third party Financial Institution or DNFBP located in a high risk country or jurisdiction, is solely mitigated by the group's anti-money laundering, countering the financing of terrorism and financing of proliferation of weapons of mass destruction internal policies, controls and oversight mechanisms.

50. In rules 47, 48, and 49 relying on third party Financial Institution or DNFBP shall not mean outsourcing or agency relationships.

Information Sharing

51. (1) A DNFBP may share with another DNFBP any information obtained in the course of carrying out CDD measures under paragraphs (a) to (d) of subsection (5) of section 2 of the Act in any of the circumstances specified in paragraphs (a) to (e) of subsection (4) of section 2 of the Act, where that DNFBP has identified the risk, in relation to any transaction, regardless of any exemption granted or any threshold specified under the Act.

(2) Every DNFBP that receives or provides information under this rule shall ensure that-

(a) appropriate measures are taken to ensure the confidentiality, integrity and security of such information;

(b) the information is used solely for purposes of CDD, risk profiling, or compliance with obligations relating to the anti-money laundering, countering the financing of terrorism and financing of proliferation of weapons of mass destruction;

(c) such information is not disclosed to any other person except as permitted under the Act or these rules; and

(d) documented policies, procedures and controls are in place to receive, provide, record and manage such information.

PART III

TARGETED FINANCIAL SANCTIONS

52. (1) Every DNFBP shall verify whether a prospective or existing customer, including any beneficial owner, director, authorized person of such customer, occasional customer, beneficiary of a transaction and, any agent and vendor of such DNFBP -

(a) appears on any list of designated person, group or entity;

(b) acts on behalf of or under the direction of any designated person, group or entity; or

(c) is owned or controlled by or acting for the benefit of any designated person, group or entity.

(2) Every DNFBP shall, in complying with targeted financial sanctions under any Order issued by the Competent Authority in terms of regulations made under the United Nations Act, take freezing action without delay and without prior notice to the customer.

(3) Every DNFBP shall in complying with targeted financial sanctions, lift such freezing action without delay-

(a) where any person, group or entity is no longer a designated person, group or entity; or

(b) upon receipt of communication from the competent authority to that effect and take measures to inform such person, group or entity forthwith.

53. Every DNFBP shall, forthwith and periodically as the case may be, verify whether any of its existing business relationships, employees, vendors and agents are held or linked to any designated person, group or entity.

54. (1) Every DNFBP shall report to the Competent Authority any assets frozen and any attempted transaction, and actions taken in compliance with the prohibition requirements under any regulation made in terms of the United Nations Act, giving effect to United Nations Security Council Resolutions on targeted financial sanctions related to prevention and suppression of terrorism and terrorist financing and prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing or in terms of any other regulation made under the United Nations Act giving effect to any other related United Nations Security Council Resolution.

(2) For the purpose of this rule, the "Competent Authority" means the Competent Authority appointed under any regulation made in terms of the United Nations Act, giving effect to United Nations Security Council Resolutions on targeted financial sanctions related to prevention and suppression of terrorism and terrorist financing and prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing or in terms of any other regulation made under the United Nations Act giving effect to any other related United Nations Security Council Resolution.

PART IV

RECORD KEEPING

55. Every DNFBP shall maintain all records -

(a) of transactions, both domestic and international, including the results of any analysis undertaken, such as inquiries to establish the background and purpose of complex or unusually large transactions;

(b) of correspondence relating to all transactions;

(c) obtained or created as a part of CDD processes in terms of section 2 of the Act and these rules including documents used to verify the identity of customers and beneficial owners, results of any analysis undertaken, risk assessments and customer account files and correspondence relating to business or professional relationships; and

(d) of reports furnished to the Financial Intelligence Unit.

for a minimum period of six years from the date of completion of transaction, correspondence, closure of business relationships and reporting to the Financial Intelligence Unit, as the case may be.

56. The records shall be sufficient to permit reconstruction of individual transactions including the nature and date of the transaction, the type and amount of currency involved and the type and identifying number of any account involved

in the transaction so as to be produced in a court of law, where necessary, as evidence. The transaction records may be maintained in document form, by electronic means, on microfilm or in any other form that may be admissible as evidence in a court of law.

57. (1) Every DNFBP may maintain records in a machine-readable form, electronic form and in the form of an audio or video recording, and be kept in its original form or copy with the DNFBP's authentication:

Provided however, in the case of non-resident customers, the DNFBP shall obtain a copy of such record as authenticated by the person who is authorized to authenticate such records in such country or jurisdiction, including the following:-

(a) a company registrar or similar authority in the country where the documents were originally issued;

(b) a Sri Lankan diplomatic officer or Sri Lankan consular officer in the country where the documents were originally issued;

(c) a solicitor, lawyer, a notary practicing in the country or jurisdiction of the non-resident customer.

(2) Such records shall be maintained up-to-date and in a readily retrievable manner.

58. Every DNFBP shall retain the records for a longer period where customers, accounts or transactions are involved in litigation or are required to be produced in a court of law or before any other relevant authority.

59. (l) Every DNFBP shall ensure that all records maintained under paragraphs (a) to (d) of rule 55 are made available immediately to the competent authorities, supervisory authorities and the Financial Intelligence Unit, upon request.

(2) For the purposes of this rule relevant domestic authorities mean-

(a) any public authority, including a supervisory authority established as an independent non-governmental authority with statutory powers, entrusted with responsibilities for combating money laundering, terrorist financing, or proliferation financing and includes the competent authority as defined in the Act;

(b) any authority that performs the functions of investigating, prosecuting or proceedings in respect of an act constituting the offence of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction or any other unlawful activity and seizing or freezing and confiscating assets relating to such offences and unlawful activities; and

(c) any authority receiving reports on cross-border transportation of currency and bearer negotiable instruments.

PART V

MISCELLANEOUS

60. The provisions of the Electronic Transactions Act, No. 19 of 2006 may apply in respect of maintaining, retaining, obtaining, presenting, issuing, filling, granting, receiving, submitting, furnishing or collecting documents under these rules.

61. The Designated Non-Finance Business (Customer Due Diligence) Rules, No. 1 of 2018 published in the Gazette Extraordinary No. 2053/20 dated January 10, 2018, is hereby rescinded without prejudice to anything previously done thereunder.

62. In these Rules –

"Act" means the Financial Transactions Reporting Act, No. 6 of 2006;

"beneficial owner" shall have the same meaning assigned to it in the Act;

"Board of Directors" in relation to a DNFBP incorporated outside Sri Lanka means the senior management of such DNFBP ;

"close associate" includes –

(a) a natural person having joint beneficial ownership of a legal person or legal arrangement, or any other close business relationship or having any material interest thereto; and

(b) a legal person or legal arrangement whose beneficial owner is a natural person and is known to have been set up for the benefit of such person or his immediate family members;

"customer" shall have the same meaning assigned to it in the Act;

"designated person, group or entity" means any person, group or entity appearing on any list of designated person, group or entity issued under any regulation made under the United Nations Act, giving effect to United Nations Security Council Resolutions on targeted financial sanctions for the prevention and suppression of terrorism and terrorist financing and the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing or in terms of any other regulation made under the United Nations Act for the purpose of giving effect to any other related resolutions of the United Nations Security Council Resolution;

"event - driven review" means carrying out of CDD measures when a significant or material change occurs in the customer profile or the customer relationship with (e.g. changes in ownership, control, directors, business activity, account usage, politically exposed person status);

"existing customer" means a customer who has commenced a business or professional relationship on or before these rules come into force;

"family member" includes the spouse, children and their spouses, parents, siblings;

"Financial Action Task Force" shall have the same meaning assigned to it in the Act;

"Financial Institutions" any person engaged in or carrying out any finance business within the meaning of finance business under the Act;

"group of companies" means a group of companies, other than a financial group of companies, that consists of a parent company or other type of a legal person, exercising control and coordinating function over the rest of the group, for the application of group supervision under the anti-money laundering and countering the financing of terrorism and financing of proliferation of weapons of mass destruction policies and procedures, together with branches and subsidiaries that are subject thereto;

"legal arrangement" means a legal arrangement whether it has legal personality or not and includes an express trust, a fiduciary account or a nominee;

"legal person" means any entity other than a natural person that is able to establish a permanent customer relationship with a DNFBP or otherwise owns property and includes a company, a body corporate, a foundation, a partnership or an association;

"money laundering" means the offence of money laundering in terms of section 3 of the Prevention of Money Laundering Act, No 5 of 2006;

"person" shall have the same meaning assigned to it in the Act;

"politically exposed person" means -

(a) individuals who are or have been entrusted with prominent public functions by a foreign country, such as Heads of State or of government, a politician, a senior government officer, political party officials, judicial or military officials, senior executives of state-owned corporations;

(b) individuals who are or have been entrusted domestically with prominent public functions, such as Heads of State or of government, a politician, a senior government officer, political party officials, judicial or military officials, senior executives of state-owned corporations; and

(c) persons who are or have been members of senior management of an international organization, such as directors, deputy directors and members of the board or equivalent functions;

but does not include middle ranking, or junior ranking individuals in the categories specified in paragraphs (a), (b) and (c).

"risk-based approach" means the risk-based approach in terms of section 2 of the Act;

"suspicious transaction report" shall have the same meaning assigned to it in the Act;

"terrorist financing" means an act constituting an offence connected with the financing of terrorism under the Convention on the Suppression of Terrorist Financing Act, No. 25 of 2005;

"threshold report" means a report under section 6 of the Act;

"United Nations Act" means the United Nations Act, No. 45 of 1968;

"unlawful activity" shall have the same meaning assigned to it in the Prevention of Money Laundering Act, No. 5 of 2006;

[Rule 22]

Schedule

1. Individual Customers:

(a) the following information shall be obtained:-

(i) full name as appearing in the valid identification document (e.g. valid national identity card, valid passport, or valid driving license);
(ii) national identification number or similar identification number;
(iii) date of birth;
(iv) nationality;
(v) permanent address;
(vi) residential address;

(vii) purpose of the account;
(viii) source of funds;
(ix) source of wealth, as necessary;
(x) expected modes of transaction (e.g. cash, cheque, etc.);
(xi) contact details (e.g. telephone numbers, fax numbers, e-mail address, etc.);
(xii) occupation including details of employment; and
(xiii) Tax Identification Number (TIN) (if applicable).

(b) the following documents shall be obtained (each shall be verified against the original and authenticated as specified in rule 57)-

(i) copy of identification document (*e.g*. valid national identity card, valid passport, or valid driving license); and
(ii) copy of the valid visa or permit in the case of non-resident customers.

2. Sole Proprietorships and Partnerships:

(a) the following information shall be obtained:-

(i) full name of the business as appearing in the business registration document;
(ii) full names of the proprietors and partners;
(iii) identification details of the proprietors and partners as in the case of individual customers;
(iv) nature of the business;
(v) purpose of the business or professional relationship;
(vi) registered address and the principal place of business;
(vii) source of funds;
(viii) expected modes of transaction (e.g. cash, cheque, etc.);
(ix) contact details (e.g. telephone numbers, fax numbers, e-mail address, etc.);
(x) Tax Identification Number (TIN) (if applicable);
(xi) the extent of ownership controls; and
(xii) other connected business interests.

(b) The following documents shall be obtained (each shall be verified against the original and authenticated as specified in rule 57):-

(i) copy of the business registration document;
(ii) partnership deed or agreement; and
(iii) copies of identification and address verification documents as specified in Item 1 (b).

3. Public or private corporations and companies:

(a) the following information shall be obtained:-

(i) registered name;
(ii) type of legal entity and registration number;
(iii) registered address and the principal place of business;
(iv) nature of the business;

(v) full name, date of birth, identification number and nationality of each director;

(vi) identify each shareholder with equity interest of more than ten *per cent*;

(vii) full name, nationality, date and place of birth, national identification or similar number and document type, residential address and Tax Identification Number (TIN) of each beneficial owner.

(viii) full name, date of birth, identification number and nationality of each signatory;

(ix) purpose of business or professional relationship including products, services and delivery channels;

(x) mailing address, if any;

(xi) source of funds;

(xii) expected modes of transaction (e.g. cash, cheque, etc.);

(xiii) expected types of counterparties (if applicable);

(xiv) contact details (e.g. telephone numbers, fax numbers, e-mail address, etc.);

(xv) Tax Identification Number (TIN) (if applicable);

(xvi) list of subsidiaries and affiliates.

Note: In the case of companies listed on the Colombo Stock Exchange licensed under the Securities and Exchange Commission of Sri Lanka Act, No. 19 of 2021 or any other stock exchange subject to disclosure requirements ensuring adequate transparency of beneficial ownership, DNFBPs may use the information available on such exchanges to identify the directors and shareholders.

(b) the following documents registered with registrars of companies in or outside Sri Lanka shall be obtained (each shall be verified against the original and authenticated as specified in rule 57):-

(i) copy of the Business Registration or Certificate of Incorporation;

(ii) copy of registered address;

(iii) copy of the certificate to commence business if a public quoted company;

(iv) copy of details of particulars of Directors and Secretary;

(v) copy of details of Beneficial Owners;

(vi) copy of Annual Returns;

(vii) Shareholders' details with equity interest more than ten *per cent*;

(viii) copy of Articles of Association;

(ix) Board Resolution authorizing the opening of the account;

(x) Board Resolution appointing the authorized signatories to operate the business or professional relationship;

(xi) copies of identification documents of authorized signatories;

(xii) audited financial statements, as applicable; and

(xiii) copy of any other document deemed necessary by the DNFBP.

4. Trusts or similar arrangements:

(a) In the case of a trust or similar arrangement, including Waqfs, created or governed under any law of Sri Lanka, the following information shall be obtained:-

(i) registered name and number of such trust or similar arrangement;

(ii) registered address as appearing in the Instrument of such trust or similar arrangement (e.g. trust deed);

(iii) purpose of such trust or similar arrangement;

(iv) identification details (full name and identification number) of the settlor or author, trustees, beneficiaries,

and any other natural person exercising ultimate effective control over such trust or similar arrangement;

(v) sufficient information to satisfy the DNFBP that it will be able to establish the identity of the class of beneficiaries at the time of payout or when the beneficiary intends to exercise vested rights;

(vi) whether the customer is the author of such trust or similar arrangement or a trustee or any other person engaged in the execution of such trust or similar arrangement such as an agent, a legal representative, a manager, an investment advisor, or a tax advisor, an accountant, other intermediary or otherwise; If any or all of those persons are legal persons, then, information on such persons, in accordance with Item 3 of this Schedule and legal arrangements in accordance with this Item;

(vii) details of the property of such trust or similar arrangement; (e.g. land, cash, vehicle, etc.);

(viii) source of funds;

(ix) expected modes of transaction (e.g. cash, cheque, etc.);

(x) expected types of counterparties (if applicable);

(xi) Tax Identification Number (TIN) of such trust or similar arrangement (if applicable).

(b) In the case of a trust or similar arrangement referred to in paragraph (a), the following documents shall be obtained (each shall be verified against the original and authenticated as specified in rule 57) :-

(i) copy of the Instrument of trust or similar arrangement, as applicable, and if not available, a written statement or declaration from the trustee[s] as to the terms of such trust or similar arrangement;

(ii) copy of the Order under section 114 of the Trust Ordinance No. 9 of 1917 (if applicable);

(iii) copy of the certificate of registration issued by the Registrar-General of Lands appointed under section 2 of the Registration of Documents Ordinance (Chapter 117);

(iv) copies of identification documents of settlor or author, trustees, beneficiaries, and any other natural person exercising ultimate effective control over the trust or similar arrangement and individuals that are part of the trust or similar arrangement.

(c) In the case of a trust or similar arrangement created or governed under a law of a foreign jurisdiction, the following information shall be obtained:-

(i) registered name and registered number (if available) of such trust or similar arrangement;

(ii) jurisdiction under which it was created or is governed;

(iii) the governing law of such trust or similar arrangement;

(iv) the purpose of such trust or similar arrangement and its connection to Sri Lanka;

(v) identification details (full name, nationality and identification number) of the settlor or author, trustees, beneficiaries, and any other natural person exercising ultimate effective control over the trust or similar arrangement;

(vi) source of funds;

(vii) expected types of counterparties (if applicable);

(viii) sufficient information to satisfy the DNFBP that it will be able to establish the identity of the class of beneficiaries at the time of payout or when the beneficiary intends to exercise vested rights;

(ix) whether the customer is the author of such trust or similar arrangement or a trustee or any other person engaged in the execution of such trust or similar arrangement such as an agent, a legal representative, a manager, an investment advisor, or a tax advisor, an accountant, other intermediary or otherwise; If any or all of those persons are legal persons, then, information on such persons, in accordance with Item 3 of this Schedule; and information on legal arrangements in accordance with this Item;

(x) details of such trust or similar arrangement property (e.g. land, cash, vehicle, etc.).

(d) In the case of a trust or similar arrangement referred to in paragraph (c), the following documents shall be obtained (each shall be verified against the original and authenticated as specified in rule 57):-

(i) copy of the Instrument of trust or similar arrangement, or similar document of such trust or similar arrangement; a certified translation where the trust deed or similar document is not available in English;

(ii) copy of certificate of registration or similar document;

(iii) copies of identification documents of settlor or author, trustees, beneficiaries, and any other natural person exercising ultimate effective control over the trust or similar arrangement, and individuals that are part of the trust or similar arrangement;

(iv) such other reliable documentation as may be required by the DNFBP to satisfy itself as to the existence, ownership, control structure, and purpose of the trust or similar arrangement.

5. Non-Governmental Organizations, Not-for-Profit Organizations, clubs, societies, associations or charitable institutions:

(a) the following information shall be obtained:-

(i) registered name and number of the institution;

(ii) registered address;

(iii) general objects;

(iv) purpose of business or professional relationship;

(v) full names, dates of birth, identification numbers, nationalities, permanent and residential addresses, at least of two office bearers, signatories, administrators, members of the governing body or committee or any other person who has control and influence over the operations of the entity;

(vi) source of funds;

(vii) expected modes of transactions (e.g. cash, cheque, etc.);

(viii) expected types of counterparties (if applicable);

(ix) other connected institutions, associations, organizations;

(x) contact details (e.g. telephone numbers, fax numbers, e-mail address, etc.);

(xi) Tax Identification Number (TIN) (if applicable).

(b) the following documents shall be obtained (each shall be verified against the original and authenticated as specified in rule 57) :-

(i) copy of the registration document;

(ii) copy of the constitution or charter etc.;

(iii) resolution authorizing the establishment of the relationship or transaction and appointing of authorized signatories;

(iv) copies of identification documents of persons specified in Item (5)(a)(v) (e.g. valid national identity card, valid passport, or valid driving license).

PRINTED AT THE DEPARTMENT OF GOVERNMENT PRINTING, SRI LANKA.