ශ්‍රී ලංකා ප්‍රජාතාන්ත්‍රික සමාජවාදී ජනරජයේ ගැසට් පත්‍රය

අති විශෙෂ

The Gazette of the Democratic Socialist Republic of Sri Lanka

EXTRAORDINARY

අංක **2511/51 - 2026** ඔක්තෝබර් මස **22** වැනි බ්‍රහස්පතින්දා - **2026.10.22**

No. 2511/51 - 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,
19th October, 2026.

Rules

1. These rules may be cited as the Financial Institutions (Customer Due Diligence) Rules, No.1 of 2026.

2. These rules shall apply to any person engaged in or carrying out any finance business within the meaning of the Act (hereinafter referred to as the "Financial Institution").

1A - G 48292 - 33 (10/2026)
This Gazette Extraordinary can be downloaded from www.documents.gov.lk

PART I

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

3. Every Financial Institution 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 Financial Institution's activities and its risk profile by applying a risk-based approach.

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

(a) obtain approval of the Board of Directors for the risk appetite and the risk tolerance level of the Financial Institution;

(b) 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;

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

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

(e) advise the Board of Directors of such risk assessment and the measures to manage the risk;

(f) obtain the approval of the Board of Directors for such risk assessment and any update thereto; and

(g) provide risk assessment information to the relevant supervisory authority or the Financial Intelligence Unit as the case may be.

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

6. A Financial Institution's risk management shall be integrated with the enterprise-wide risk management of the Financial Institution.

7. Every Financial Institution 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 of the Financial Institution as specified in rule 14(d); and

(d) timely reporting to the Board of Directors as specified in rule 11;

8. (1) Every Financial Institution 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 Financial Institution may conduct risk profiling of occasional customers under these rules if the need arises.

(3) Every Financial Institution may use the information obtained under rule 21 for the purpose of considering the matters specified in sub rule (1) of this rule for initial risk profiling.

9. The risk control and mitigation measures implemented by every Financial Institution in relation to its customers shall be commensurate with the customer's risk profile conducted under rule 8.

10. Every Financial Institution shall-

(a) prior to establishing a business relationship with a customer, comply with the provisions of rule 21; and

(b) upon the initial acceptance of a customer, periodically conduct due diligence review in accordance with rule 33 and update the customer's risk profile based on the current level of risk of such customer.

11. (1) Every Financial Institution 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. 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 Financial Institution for combating the risk (such as the level of the Financial Institution'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, business 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 Financial Institution;

(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 Financial Institution; and

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

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

12. (1) Every Financial Institution shall formulate an internal policy approved by its Board of Directors 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 Financial Institution, 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.

(2) The detailed procedures, controls and systems shall be developed by each Financial Institution in compliance with such policy and be approved by the 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 wire transfers and 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 relationship.

13. Every Financial Institution 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 Financial Institution shall -

(a) provide the compliance officer appointed in terms of the provisions of the Act, with sufficient resources to ensure the duties, functions and obligations of the Financial Institution under the Act and these rules are performed and discharged;

(b) 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;

(c) 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;

(d) design and implement, on-going, periodic training and awareness programmes for employees including the Board of Directors, 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

(e) maintain an independent audit function that is adequately resourced and able to regularly assess the effectiveness of the Financial Institution'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 Financial Groups

15. Every financial group 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 financial 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 and controls for sharing information within the financial group 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 financial 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 financial 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.

16. (1) Every Financial Institution shall ensure that its foreign branches and majority-owned subsidiaries 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 Financial Institution 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.

Use of New Technologies

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

(2) Every Financial Institution shall-

(a) undertake a risk assessment prior to the launch or use of such new products, services, business 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 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 Financial Institution 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, or any account which to the knowledge of the Financial Institution 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 Financial Institution and accounts that are operated and maintained with the account holder's name omitted.

19. (1) Every Financial Institution shall maintain information in such a manner that the accounts, records and information in relation to assets and liabilities of a given customer of such Financial Institution can be readily retrievable.

(2) A Financial Institution shall not maintain accounts separate from the Financial Institution's standard operational processes, controls, systems or procedures.

20. Every Financial Institution shall conduct CDD measures specified in these rules, when :–

(a) establishing a business relationship;

(b) carrying out occasional transactions being wire transfers as referred to in rules 61 to 75;

(c) carrying out occasional transactions, including carrying out money and currency buying, selling or exchanging, involving an amount exceeding Sri Lanka Rupees two hundred thousand 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;

(d) the Financial Institution has any suspicion or has reasonable grounds to believe that the 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

(e) the Financial Institution has any doubt about the veracity or adequacy of customer identification documents or information already obtained.

21. Every Financial Institution in conducting CDD measures under these rules shall obtain up-to date and accurate information specified in Schedule I 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 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 8;

(f) conduct ongoing due diligence throughout the course of the business 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 relationship.

22. Where a Financial Institution is unable to comply with CDD measures specified in these rules, such Financial Institution shall –

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

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

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

23. Where a Financial Institution 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 Financial Institution is permitted not to conduct CDD measures and shall immediately make a suspicious transaction report.

Risk Based Due Diligence

24. Without prejudice to the provisions of rule 21, where any customer is rated as a customer posing a low risk, the Financial Institution may conduct simplified CDD measures specified in Schedule II hereto, as the Financial Institution may deem appropriate, but not limited to, the measures specified in Schedule II.

25. (1) Where any customer is rated as a customer posing a high risk, the Financial Institution shall conduct enhanced CDD measures for such customer, as specified in Schedule III hereto, in addition to the CDD measures specified in rule 21 and any other measures as the Financial Institution may deem necessary.

(2) Every Financial Institution shall, in conducting the enhanced CDD measures specified in Schedule III, determine the appropriate measures applicable to each and every customer.

Delayed Verification

26. Every Financial Institution shall verify the identity of the customer and beneficial owner prior to or during the course of establishing a business 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 relationship, the Financial Institution 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 relationship;

(b) the delay shall be essential so as not to interrupt the Financial Institution'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.

27. Every Financial Institution shall take measures to mitigate the risk of delayed verification, including recording the conditions under which the customer may utilise the business 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 account behaviour.

28. A Financial Institution shall not, under any circumstances, establish a business relationship, open an account 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

29. Every Financial Institution shall monitor all business 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 Financial Institution's knowledge of such customer.

30. (1) Every Financial Institution 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.

31. Every Financial Institution shall increase the number and timing of controls applied and select patterns of transactions that need further examination, in relation to high risk business relationships.

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

33. (1) Every Financial Institution 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 Financial Institution, 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 adverse media screening; 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 Financial Institution 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 Financial Institution shall ensure that periodic reviews are completed on or before the next periodic review cycle date.

34. Every Financial Institution 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 Financial Institution 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 Financial Institution 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 relationship is operated; or

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

36. Every Financial Institution 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.

Third Party Customers

37. Every Financial Institution shall with regard to all transactions including cash deposits exceeding Sri Lanka rupees two hundred thousand or its equivalent in any foreign currency deposited into an account separately or in aggregate by a third party customer, have on record the name, address, identification number of a valid identification document, purpose and the signature, where applicable, of the third party customer:

Provided however, clerks, accountants, employees, agents, or authorized persons of business places who are authorized to deal with the accounts shall not be considered as a third party customer.

Legal Persons and Legal Arrangements

38. Every Financial Institution 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 I hereto.

39. (1) In order to identify the beneficial owner in a legal person a Financial Institution 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 Financial Institution shall, identify and take reasonable measures to verify the natural person who controls such other legal person or legal arrangement.

40. In order to identify the beneficial owner in a legal arrangement, a Financial Institution 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

41. Every Financial Institution shall, in addition to the other provisions of these rules, conduct CDD measures when entering into a business 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.

42. (1) Every Financial Institution shall open accounts in the name of the relevant NGO, NPO or charitable institution as per the title given in their constituent documents.

(2) 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.

43. A Financial Institution shall not allow personal accounts of the members of the governing bodies of a NGO, NPO or charitable institution to be used for the objectives and purposes of such NGO, NPO or charitable institution.

44. Every Financial Institution 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 99.

Business Relationships or Transactions where the customer is not physically present

45. (1) Every Financial Institution may establish a non- face to face business relationship or conduct a non- face to face transaction with a customer, only if such Financial Institution has policies, procedures and controls in place to address any specific risk associated with such business 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 relationships and transactions;
(b) controls in order to avoid the risk posed in establishing and conducting business relationships or transactions through information and communication technology; and

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

Beneficiaries of Insurance Policies

46. (1) Every Financial Institution shall in addition to the CDD measures required for a customer and a beneficial owner, conduct the following CDD measures on the beneficiary of a life insurance and other investment related insurance policy, as soon as the beneficiary is identified or designated:-

(a) in the case of a beneficiary that is identified as specifically named natural or legal person or legal arrangement, obtain the name of the natural or legal person or legal arrangement;

(b) in the case of a beneficiary that is designated by characteristics or by class or by other means, obtain sufficient information concerning the beneficiary to satisfy the Financial Institution that it will be able to establish the identity of the beneficiary at the time of pay-out.

(2) In the case of a beneficiary referred to in paragraphs (a) and (b) of sub rule (1), the verification of the identity of the beneficiary shall occur at the time of the pay-out.

47. Every Financial Institution shall consider the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are required. If the Financial Institution determines that a beneficiary who is a legal person or a legal arrangement presents a high risk, it shall conduct enhanced CDD measures which shall include reasonable mechanisms to identify and verify the identity of the beneficial owner of the beneficiary, at the time of pay-out.

Customers from high risk Countries or Jurisdictions

48. (1) Every Financial Institution shall apply effective enhanced CDD measures that shall correspond to the risk to business relationships and transactions with customers and Financial Institutions 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.

49. Every Financial Institution shall, in addition to enhanced CDD measures, apply appropriate counter measures, for high risk countries or jurisdictions referred to in sub rule (2) of rule 48, corresponding to the nature of the risk of such high risk countries or jurisdictions, as follows:-

(a) limiting business relationships 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 Financial Institutions in high risk countries or jurisdictions;

(c) reviewing, amending or terminating, if necessary, correspondent banking relationships with Financial Institutions 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 Financial Institution or financial group 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)

50. (1) Every Financial Institution 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 Financial Institution shall-

(a) obtain approval from the Board of Directors of the Financial Institution to enter into or continue the business 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;

(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 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.

51. In relation to life insurance policies or other investment related insurance policies, of politically exposed persons, every Financial Institution shall-

(a) take reasonable measures to determine whether the beneficiary, or the beneficial owner of the beneficiary, as the case may be, is a politically exposed person, at the time of appointment or pay-out; and

(b) where a high risk is identified, inform the senior management before the pay-out of the policy proceeds, scrutinize the whole business relationship with the policy holder, and consider whether to make a suspicious transaction report.

Financial Institutions which rely on Third Parties

52. (1) A Financial Institution may rely on a third party Financial Institution or designated non-finance business or profession 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 relationship or to introduce business.

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

(a) obtain immediately the necessary information relating to the CDD measures undertaken by the third party Financial Institution or designated non-finance business or profession;

(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 designated non-finance business or profession without delay, upon request; and

(c) satisfy itself that such third party Financial Institution or designated non-finance business or profession 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.

53. Every Financial Institution which relies on a third party Financial Institution or designated non-finance business or profession 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 designated non-finance business or profession.

54. Where a Financial Institution acting in accordance with rule 52 or 53 relies on a third party Financial Institution or designated non-finance business or profession that forms part of the same financial group or group of companies, such Financial Institution 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 designated non-finance business or profession located in a high risk country or jurisdiction referred to in rule 48, 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.

55. In rules 52, 53 and 54 relying on third party Financial Institution or designated non-finance business or profession shall not mean outsourcing or agency relationships.

Information Sharing

56. (1) A Financial Institution may share with another Financial Institution 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 Financial Institution has identified the risk, in relation to any transaction, regardless of any exemption granted or any threshold specified under the Act.

(2) Every Financial Institution 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

CORRESPONDENT BANKING

57. (1) Every Financial Institution providing correspondent banking services or other similar banking services (hereinafter referred to as "correspondent bank") to respondent institutions, shall take necessary measures to ensure that the risk arising from or associated with the relationship with the respondent institution (e.g. being used by shell banks) are duly managed.

(2) Every correspondent bank shall assess the suitability of the respondent institution by taking the following measures in addition to performing due diligence: -

(a) gather adequate information about the respondent institution, to thoroughly understand the nature of the respondent institution's business, including the following: -

(i) internal policy of the respondent institution on anti-money laundering, countering the financing of terrorism and financing of proliferation of weapons of mass destruction;

(ii) information about the respondent institution's management and ownership;

(iii) core business activities;

(iv) country of geographical presence, jurisdiction or country of correspondence;

(v) risk prevention and detection measures;

(vi) the purpose of the account or service;

(vii) reputation of the respondent institution through publicly available sources, as far as practicable; and

(viii) the quality of supervision of the respondent institution, including whether it has been subject to money laundering, terrorist financing or financing of proliferation of weapons of mass destruction investigations or regulatory actions;

(b) assess the respondent institution's anti-money laundering and countering the financing of terrorism and financing of proliferation of weapons of mass destruction controls and ascertain whether they are adequate and effective; and

(c) clearly understand and record the respective anti-money laundering, countering the financing of terrorism and financing of proliferation of weapons of mass destruction responsibilities of each institution.

(3) Every correspondent bank shall obtain approval of its Board of Directors before entering into new correspondent banking relationships.

58. Every correspondent bank shall in relation to "payable-through accounts", satisfy itself that the respondent institution -

(a) has conducted CDD measures on its customers that have direct access to the accounts of the correspondent bank; and

(b) is able to provide relevant CDD information upon request to the correspondent bank.

59. Every correspondent bank shall apply enhanced CDD measures when entering into or continuing correspondent banking relationships with respondent institutions which are located in high risk countries or jurisdictions, referred to in rule 48.

60. (1) A correspondent bank shall not enter into or continue a correspondent banking relationship with a shell bank.

(2) When providing correspondent banking services, every correspondent bank shall take appropriate measures to satisfy itself that its respondent institutions do not permit their accounts to be used by shell banks.

PART IV

CROSS-BORDER PAYMENTS, DOMESTIC PAYMENTS OR VALUE TRANSFERS

61. Every Financial Institution shall, in processing cross-border payments, domestic payments or value transfers conducted through wire transfers (in these rules referred to as "wire transfers"), take freezing action and comply with prohibitions on conducting transactions with -

(a) any designated person, group or entity;

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

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

62. Every Financial Institution shall monitor all wire transfers to detect transactions which lack the relevant originator or beneficiary information as required by rule 64 and rule 65 and take appropriate measures to ensure all required information is obtained.

63. Every Financial Institution shall ensure that account numbers or any other information contained in wire transfers is not used to disguise the country where the Ordering or Beneficiary Financial Institution is located.

Ordering Financial Institutions

64. (1) Every Ordering Financial Institution shall ensure that wire transfers equal to or above United States Dollars Thousand (USD 1000) or its equivalent in any foreign currency or Sri Lanka Rupees, including batch transfers, are always accompanied with:-

(a) the following originator information -

(i) name;

(ii) in the case of a natural person, national identity card number or any other customer identification number and the date of birth;

(iii) in the case of a legal person, company or business registration number;

(iv) address;

(v) originating account number where such 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

(vi) where the originating account referred to in sub paragraph (v) is not used and funds are drawn from another Financial Institution other than the Ordering Financial Institution, the account number and the name of such Financial Institution from where the funds are drawn; and

(b) the following beneficiary information -

(i) name;

(ii) beneficiary account number where such 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;

(iii) in the case of a legal person, company or business registration number; and

(iv) name of country and town.

(2) Every Ordering Financial Institution shall verify the information referred to in sub rule (1)(a), for accuracy.

65. (1) Every Ordering Financial Institution shall ensure that wire transfers below United States Dollars Thousand (USD 1000) or its equivalent in Sri Lanka Rupees or any foreign currency, including batch transfers, are always accompanied with:-

(a) the following originator information -

(i) name;

(ii) 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) where the originating account referred to in sub paragraph (ii) is not used and funds are drawn from another Financial Institution other than the Ordering Financial Institution, the account number and the name of such Financial Institution from where the funds are drawn; and

(b) the following beneficiary information -

(i) name;

(ii) 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) Every Ordering Financial Institution-

(a) may verify the information referred to in sub rule (1)(a) for accuracy;

(b) shall verify the information pertaining to its customer where there is a suspicion or it 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.

66. (1) Where the information accompanying the domestic wire transfer can be made available to the Beneficiary Financial Institution and appropriate authorities by other means, the Ordering Financial Institution shall include the account number or a unique transaction reference number, provided that any such number will permit the transaction to be traced back to the originator or the beneficiary.

(2) The Ordering Financial Institution shall, after receiving the request either from the Beneficiary or Intermediary Financial Institution or from the appropriate authority, make the information available within three working days.

67. If any Ordering Financial Institution fails to comply with the requirements specified in rules 64 and 65 in respect of a wire transfer, such Financial Institution shall not proceed with the wire transfer and shall consider making a suspicious transaction report.

Intermediary Financial Institution

68. Every Financial Institution involved in wire transfers as an Intermediary Financial Institution shall ensure that all originator and beneficiary information that accompanies a wire transfer is retained with the wire transfer message.

69. 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 six years, of all the information received from the Ordering Financial Institution or another Intermediary Financial Institution.

70. Every Intermediary Financial Institution shall take reasonable measures, which are consistent with straight through processing to identify wire transfers that lack required originator and required beneficiary information.

71. Every Intermediary Financial Institution shall have risk-based internal policies and procedures in relation to -

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

(b) the appropriate follow up action.

Beneficiary Financial Institution

72. Every Beneficiary Financial Institution shall take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify wire transfers that lack required originator and beneficiary information.

73. For wire transfers above United States Dollars Thousand (USD 1000) or its equivalent in Sri Lanka Rupees or any foreign currency, a Beneficiary Financial Institution shall verify the identity of the beneficiary, and maintain the information in accordance with the Act and these rules, if the identity has not been previously verified.

74. Every Beneficiary Financial Institution shall, in relation to wire transfers above the amount specified in rule 73, take measures to mitigate the risk of transfers being made to an unintended beneficiary, including at least one of the following:-

(a) for each transaction, check the extent to which the name and account number of the beneficiary in the payment message aligns with the information held by such Beneficiary Financial Institution;

(b) conduct ongoing monitoring to identify anomalous accounts, transactions, and activity, including misaligned beneficiary information, following a risk-based approach; or

(c) ensure the name and account number of the beneficiary in the payment message aligns with the information held by the Beneficiary Financial Institution where the Beneficiary and Ordering Financial Institutions both participate in a pre-validation mechanism for each transaction.

75. Every Beneficiary Financial Institution shall have risk-based internal policies and procedures for determining-

(a) when to execute, reject or suspend a wire transfer with insufficient originator or beneficiary information or a wire transfer that is potentially a misdirected payment; and

(b) the appropriate follow up action.

Money or Value Transfer Service Providers

76. Every provider of Money or Value Transfer Service (hereinafter referred to as "MVTS") shall, in addition to the other provisions of these rules, maintain a current list of all its agents in countries in which the MVTS provider and its agents operate.

77. Every MVTS provider that uses agents shall include them in its internal policy on anti-money laundering, countering the financing of terrorism and financing the proliferation of weapons of mass destruction and monitor them in compliance with that policy.

78. Every MVTS provider when operating directly or through their agents in Sri Lanka shall comply with the provisions applicable for wire transfers in these rules, and when operating directly or through its agents in a foreign country shall comply with such similar requirements issued by the relevant authority of such foreign country.

79. In the case of a MVTS provider that controls the ordering customer as well as the beneficiary customer of a wire transfer, such MVTS provider shall –

(a) take into account all relevant information from both the ordering customer and the beneficiary customer, in order to determine whether a suspicious transaction report needs to be made; and

(b) on identifying a suspicious wire transfer, make a suspicious transaction report and to the financial intelligence unit of any country affected by a suspicious wire transfer, and make available any relevant information to the Head of the Financial Intelligence Unit.

Virtual Asset Transfers (Travel Rule)

80. (1) Every Virtual Asset Service Provider (hereinafter referred to as "VASP") shall, in addition to the other provisions of these rules, when carrying out any virtual asset transfer, comply with the requirements specified in rule 81 to rule 94.

(2) For the purpose of rule 83 to rule 94 –

(a) "Central Account Number" means the primary account which controls and manages one or more sub accounts, used and operated by a person;

(b) "Personal Identification Number" includes the National Identification Card number, passport number or personal identification number issued by the relevant authority of any country or jurisdiction, or, incorporation or registration number of any body corporate, as the case may be.

81. Every VASP, who sends or receives a virtual asset transfer to or from;

(a) an unhosted wallet; or

(b) an account or a wallet maintained by a VASP or any other entity which is not subject to CDD measures referred to in these rules, shall consider such virtual asset transfer as a high risk virtual asset transfer, conduct enhanced CDD and shall ensure that the information referred to in rule 83 and rule 86 is duly obtained and verified, as applicable, in accordance with the provisions of such rules.

82. Every VASP shall, in carrying out or facilitating any virtual asset transfer, take freezing action and comply with prohibitions on conducting transactions with -

(a) any designated person, group or entity;

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

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

Originating VASP

83. Every Originating VASP shall obtain and retain the following information:-

(a) originator's information as follows:-

(i) name (the originator's verified full name or name of the entity whether incorporated or unincorporated);

(ii) in the case of a natural person, date of birth;

(iii) in the case of a legal person, company or business registration number;

(iv) Central Account Number;

(v) account number or wallet address where such number or address is used to process the transaction;

(vi) unique transaction reference number where such reference number is used to process the transaction;

(vii) residential (geographical) address or address of the entity either incorporated or unincorporated, provided such address has been verified as part of the CDD measures by the Originating VASP, for accuracy;

(viii) Personal Identification Number;

(b) beneficiary's information -

(i) name (the name of the person who is identified by the originator as the receiver of the virtual asset transfer);

(ii) in the case of a legal person, company or business registration number;

(iii) name of the country and town;

(iv) account number or wallet address where such number or address is used to process the transaction; and

(v) unique transaction reference number where such reference number is used to process the transaction.

84. Every Originating VASP shall –

(a) securely submit forthwith the information referred to in rule 83 to the Beneficiary VASP, Intermediary VASP or Financial Institution, if any;

(b) make available such information on request to the Financial Intelligence Unit and any other appropriate authority in a timely manner.

85. Where any Originating VASP fails to comply with the requirements specified in rule 83 in respect of a virtual asset transfer, such Originating VASP shall-

(a) not proceed with such virtual asset transfer;

(b) consider reporting the relevant transaction as a suspicious transaction; and

(c) comply with any direction, guideline or circular issued by the Head of the Financial Intelligence Unit in that regard.

Intermediary VASP

86. Every VASP which is involved in any virtual asset transfer as an Intermediary VASP, shall ensure that, the required originator and beneficiary information referred to in rule 83 in respect of all virtual asset transfers carried out by such Intermediary VASP, is retained with the virtual asset transfer message or communication.

87. Every Intermediary VASP shall –

(a) securely submit forthwith the information referred to in rule 83, to the Beneficiary VASP, any other Intermediary VASP or Financial Institution, if any:

Provided however, where any technical limitation prevents an Intermediary VASP from submitting information under paragraph (a), such Intermediary VASP shall keep a record of all the information received from the originator VASP, other Intermediary VASP or Financial Institution, if any, for at least six years; and

(b) make available such information on request to the Financial Intelligence Unit and any other appropriate authority in a timely manner.

88. Every Intermediary VASP shall take reasonable measures consistent with straight through processing to identify virtual asset transfers, that lack the required originator and beneficiary information referred to in rule 83.

89. Every Intermediary VASP shall establish and maintain risk-based internal policies, procedures and controls in relation to-

(a) the execution, rejection or suspension of a virtual asset transfer lacking required originator or beneficiary or Financial Institution information, where applicable; and

(b) the appropriate follow up measures and action to be taken in respect of such transfers.

Beneficiary VASP

90. Every beneficiary VASP shall obtain and retain the following information-

(a) originator's information as follows-

(i) name (the originator's full name or name of the entity whether incorporated or unincorporated);

(ii) in the case of a natural person, date of birth;

(iii) in the case of a legal person, company or business registration number;

(iv) Central Account Number;

(v) account number or wallet address where such number or address is used to process the transaction;

(vi) unique transaction reference number where such reference number is used to process the transaction;

(vii) residential (geographical) address or address of the entity either incorporated or unincorporated; and

(viii) Personal Identification Number.

(b) beneficiary's information as follows -

(i) name of the person who is identified by the originator as the receiver of the virtual assets transfer:

Provided that, the beneficiary VASP shall verify the beneficiary's name for accuracy, if the name of the customer has not previously been verified;

(ii) in the case of a legal person, company or business registration number;

(iii) name of country and town;

(iv) account number or wallet address where such number or address is used to process the transaction; and

(v) unique transaction reference number where such reference number is used to process the transaction.

91. Every Beneficiary VASP shall take reasonable measures, which may, where feasible, include post-event monitoring or real-time monitoring, to identify virtual asset transfers that does not contain the originator or beneficiary information as required in rule 83.

92. Every Beneficiary VASP shall establish and verify the identity of the beneficiary and maintain the relevant records and information in accordance with the provisions of the Act and these rules, where the identity of such beneficiary has not been previously verified.

93. Every Beneficiary VASP shall establish and maintain risk-based internal policies, procedures and controls in relation to-

(a) the execution, rejection or suspension of a virtual asset transfer lacking required originator or beneficiary or Financial Institution information, where applicable; and

(b) the appropriate follow up measures and action to be taken in respect of such a transfer.

94. Every Beneficiary VASP shall make available information referred to in rule 90 on request to the Financial Intelligence Unit and any other appropriate authority in a timely manner.

Card Payments and Cash Withdrawals

95. Every Financial Institution shall, in relation to any transfer that originates from a transaction carried out using a credit, debit or prepaid card for the purchase of goods or services, ensure that-

(a) such transfers are accompanied by the credit, debit or prepaid card number; and

(b) the names and locations of the card issuing and merchant acquiring Financial Institutions are made available upon request in a timely manner.

96. Every Financial Institution shall, in relation to cross-border cash withdrawals using a credit, debit or prepaid card through a different Financial Institution ensure that-

(a) the card number accompanies the cash withdrawal; and

(b) the name of the cardholder is sent to the acquiring financial institution, within three business days of receiving a request.

97. Every Financial Institution shall ensure that domestic cash withdrawals are accompanied by the account number or card number.

98. Every Financial Institution shall take appropriate measures to manage and mitigate the risk that may arise through the misuse of credit cards.

PART V

TARGETED FINANCIAL SANCTIONS

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

(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 Financial Institution 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 Financial Institution 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.

100. Every Financial Institution 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.

101. (1) Every Financial Institution 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 VI

RECORD KEEPING

102. Every Financial Institution 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 business correspondence;

(d) of reports furnished to the Financial Intelligence Unit; and

(e) of Society for Worldwide Interbank Financial Telecommunication (SWIFT) messages or any other similar messages that accompany wire transfers,

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.

103. 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.

104. (1) Every Financial Institution 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 Financial Institution's authentication:

Provided however, in the case of non-resident customers, the Financial Institution 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.

105. Every Financial Institution 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.

106. (l) Every Financial Institution shall ensure that all records maintained under paragraphs (a) to (e) of rule 102 are made available immediately to relevant domestic 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 VII

MISCELLANEOUS

107. 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.

108. (1) In the case of a prospective customer whose permanent or business address given in the application is at a location far away from that of the branch which receives the account opening request, the Financial Institution shall open the account if any acceptable and valid reasons were provided and such reasons shall be kept on record.

(2) Where acceptable and valid reasons are not provided, the Financial Institution shall request the prospective customer to open the account at the closest branch to the customer's permanent address or business address.

109. Where two or more accounts of a similar category are opened in the same Financial Institution by one customer, in addition to CDD measures specified in these rules, the Financial Institution shall record the specific purpose of each such account.

110. The Financial Institutions (Customer Due Diligence) Rules, No. 1 of 2016, and published in the Gazette Extraordinary No. 1951/13 dated January 27, 2016, and the Insurers (Customer Due Diligence) Rules, No. 1 of 2019, published in the *Gazette* Extraordinary No.2123/14 dated May 13, 2019 are hereby rescinded without prejudice to anything previously done thereunder.

111. 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;

"beneficiary" means a person to whom or for whose benefit the funds are sent or deposited in or paid to a Financial Institution and may include a Beneficiary Financial Institution;

"Beneficiary Financial Institution" means an institution which receives wire transfers from the Ordering Financial Institution directly or through an Intermediary Financial Institution and makes the funds available to the beneficiary customer;

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

"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;

"collective investment schemes" shall have the same meaning assigned to it in the Securities and Exchange Commission of Sri Lanka Act, No. 19 of 2021;

"controlling interest" means an interest acquired by providing more than ten *per cent* of the capital of a legal person;

"correspondent banking" means provision of banking services by a bank (the correspondent bank) to a respondent institution including cash management (e.g large international banks frequently act as correspondent banks for large number of other banks around the world by providing a wide range of services such as interest-bearing accounts in a variety of currencies, international wire transfers, cheque clearing, payable-through accounts and foreign exchange services);

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

"domestic payments" shall include payment systems as defined in the Payment and Settlement Systems Act, No. 28 of 2005 and payment transactions;

"designated non-finance business or profession" 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 Financial Institutions (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 relationship on or before these rules come into force;

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

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

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

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

"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;

"Intermediary Financial Institution" means an institution in a 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;

"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 Financial Institution or otherwise owns property and includes a company, a body corporate, a foundation, a partnership or an association;

"majority-owned subsidiary" means a subsidiary of a group of companies of which fifty *per cent* or more of the shares are owned by the parent company;

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

"money or value transfer services" shall have the same meaning assigned to it in the Act;

"occasional customer" means any person who engages in an occasional transaction;

"occasional transaction" shall have the same meaning assigned to it in subsection (8) of section 2 of the Act;

"Ordering Financial Institution" means an institution which initiates wire transfers and transfers the funds upon receiving the request for a wire transfer on behalf of the originating customer;

"payable-through account" means correspondent accounts that are used directly by third parties to transact business on their own behalf;

"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;

"Securities and Exchange Commission" means the Securities and Exchange Commission of Sri Lanka, established under section 4 of the Securities and Exchange Commission of Sri Lanka Act, No. 19 of 2021;

"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 overall supervision. The physical presence constitutes being located within a country performing a management function with meaningful mind and the mere existence of a local agent or non-managerial staff does not constitute a physical presence;

"straight through processing" means payment transactions that are conducted electronically without need for manual intervention;

"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;

"unhosted wallet" means a virtual asset wallet or account that is not hosted or managed by a virtual asset service provider and where the user maintains exclusive control over the access keys;

"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;

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

"virtual asset service provider" shall have the same meaning assigned to it in the Act;

"wallet" means a software application, hardware device, or other technological solution that generates, stores, and manages cryptographic private keys associated with distributed ledger addresses; and

"wallet address" means a distributed ledger address registered on a distributed ledger to send, receive, and record virtual asset transfers or transactions;

Schedule I

[Rule 21]

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 (if the residential address differs from the permanent address, residential address shall be supported by a utility bill not over three months old or any other reliable proof of residence. Utility bills are to be specified as electricity bill, water bill and fixed line telephone operator's bill. No post-box number shall be accepted. In the case of 'C/o', property owner's consent and other relevant address verification documents are required to be obtained;
(vii) purpose of the account;
(viii) source of funds;
(ix) source of wealth, as necessary;
(x) expected monthly turnover;
(xi) expected modes of transaction (e.g. cash, cheque, etc.);
(xii) expected types of counterparties (if applicable);
(xiii) telephone numbers, fax numbers and e-mail address (if available);
(xiv) occupation including details of employment;
(xv) Tax Identification Number (TIN);
(xvi) in the case of non-resident customers, the reason for opening the account in Sri Lanka; and
(xvii) satisfactory reference, as applicable.

(b) the following documents shall be obtained (each shall be verified against the original and authenticated as specified in rule 104)

(i) copy of identification document (e.g. national identity card, valid passport, or valid driving license);
(ii) copy of address verification document; and
(iii) 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 relationship;
(vi) registered address and the principal place of business;
(vii) source of funds;
(viii) expected monthly turnover;
(ix) expected modes of transaction (e.g. cash, cheque, etc.);

(x) expected types of counterparties (if applicable);
(xi) telephone numbers, fax numbers and e-mail addresses;
(xii) Tax Identification Number (TIN);
(xiii) the extent of ownership controls; and
(xiv) other connected business interests;

(b) The following documents shall be obtained (each shall be verified against the original and authenticated as specified in rule 104):-

(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 relationship including products, services and delivery channels;
(x) mailing address, if any;
(xi) source of funds;
(xii) expected monthly turnover;
(xiii) expected modes of transaction (e.g. cash, cheque, etc.);
(xiv) expected types of counterparties (if applicable);
(xv) telephone, Fax, E-mail;
(xvi) Tax Identification Number (TIN);
(xvii) 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, Financial Institutions 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 104):-

(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 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 Financial Institution.

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 Financial Institution 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 transactions (e.g. cash, cheque, etc.);
(x) expected monthly turnover;
(xi) expected types of counterparties (if applicable);
(xii) 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 104) :-

(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 monthly turnover;
(viii) expected types of counterparties (if applicable);
(ix) sufficient information to satisfy the Financial Institution 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;
(x) 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;
(xi) 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 104):-

(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 Financial Institution 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 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 monthly turnover;
(viii) expected modes of transactions (e.g. cash, cheque, etc.);
(ix) expected types of counterparties (if applicable);
(x) other connected institutions, associations, organizations;
(xi) telephone number, Fax number, E-mail address;
(xii) Tax Identification Number (TIN);

(b) the following documents shall be obtained (each shall be verified against the original and authenticated as specified in rule 104) :-

(i) copy of the registration document;
(ii) copy of the constitution or charter etc.;
(iii) resolution authorizing the opening of the account 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).

6. Collective Investment Schemes, Stocks and Shares:

(a) the following shall be obtained where the customer is a collective investment scheme, mutual fund, unit trust scheme, or similar entity:-

(i) name of the approved fund;
(ii) category / type of the fund and investment purpose;
(iii) expected monthly turnover;
(iv) expected modes of transactions (e.g. cash, cheque, etc.);
(v) name of the licensed managing company;
(vi) registered address of the managing company;
(vii) whether the managing company is a regulated financial institution subject to equivalent anti-money laundering, countering terrorist financing and countering proliferation financing of weapons of mass destruction obligations.

(b) the following documents shall be obtained (each shall be verified against the original and authenticated as specified in rule 104):-

(i) copy of license or letter of approval issued to the fund by the Securities and Exchange Commission or supervisory authority of the relevant country;
(ii) copy of license issued to the managing company by the Securities and Exchange Commission or supervisory authority of the relevant country; and
(iii) copy of trust deed, management agreement, custody and administration agreement or similar.

Note: Where the customer is a managing company, the information and documentation to be obtained shall be as specified in Item 1 to Item 5 of this Schedule, as appropriate.

(c) Certification requirements for depository participants:-

For non-resident applicants all supporting documents shall be certified, attested or authenticated by the persons specified below for the purpose of validating the applicant:-

(i) by the company registrar or similar authority in the country where the documents were originally issued;
(ii) by a Sri Lankan diplomatic officer or Sri Lankan consular officer in the country where the documents were originally issued ;
(iii) by a solicitor, a lawyer, a notary practicing in the country where the applicant resides;
(iv) by the custodian bank;
(v) by the global custodian (the custodian bank shall certify the authenticity of the signature of the global custodian);or
(vi) by a broker;

(d) For resident applicants all supporting documents shall be certified, attested or authenticated by the persons specified below for the purpose of validating the applicant:-

(i) by the Registrar of Companies or the Company Secretary (applicable in respect of legal persons);
(ii) by an attorney-at-law or a notary public;
(iii) by a broker; or
(iv) by the custodian bank.

Note: (1) The person certifying shall place the signature, full name, address, contact telephone number and the official seal**.**

(2) Where the application is titled in the name of the 'Registered Holder/Global Custodian, Beneficiary" and forwarded through a custodian bank, a copy of the SWIFT message or similar document issued by the global

custodian instructing the local custodian bank to open the account on behalf of the beneficiary shall be submitted together with a declaration from the global custodian that a custody arrangement or agreement exists between the global custodian and the customer or beneficiary.

7. Specific requirements applicable to Virtual Asset Service Providers:

In the case of customers referred to in Items 1 to 5 under this Schedule where the customer is not physically present, the Internet Protocol (IP) Address shall be obtained in addition to the information and documents specified in Items 1 to 5.

Note: where the customer referred to in Items 1 to 5, is an occasional customer, a Financial Institution may obtain information on source of wealth, expected monthly turnover, expected modes of transaction, expected types of counterparties and satisfactory references.

Schedule II

[Rule 24]

Simplified CDD measures

(1) Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (delayed verification);

(2) Reducing the frequency of periodic reviews of customer relationships; and

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

Schedule III

[Rule 25]

Enhanced CDD measures

In addition to the information specified in Schedule I-

(a) the following shall be obtained and verified, 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 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 as the Financial Institution may deem necessary.

(b) the following approvals and monitoring measures shall be required -

(i) approval of senior management to commence or continue the business relationship;
(ii) enhanced monitoring of the business relationship, including increased number and timing of controls; selection and review of transaction patterns requiring further examination; and
(iii) periodic review of customer relationship within a period of one year.

PRINTED AT THE DEPARTMENT OF GOVERNMENT PRINTING, SRI LANKA.