ශ්‍රී ලංකා ප්‍රජාතාන්ත්‍රික සමාජවාදී ජනරජයේ ගැසට් පත්‍රය

අති විශෙෂ

The Gazette of the Democratic Socialist Republic of Sri Lanka

EXTRAORDINARY

අංක 1951/13 - 2016 ජනවාරි මස 27 වැනි බදාදා - 2016.01.27

No. 1951/13 - WEDNESDAY JANUARY 27, 2015

(Published by Authority)

PART I : SECTION (I) — GENERAL

Central Bank of Sri Lanka Notices

L. D. B. 3/2006

FINANCIAL TRANSACTIONS REPORTING ACT, No. 6 OF 2006

RULES made by the Financial Intelligence Unit under section 2 of the Financial Transactions Reporting Act, No.6 of 2006.

Financial Intelligence Unit.

27th January, 2016,
Colombo.

Rules

1. These Rules may be cited as the Financial Institutions (Customer Due Diligence) Rules, No. 1 of 2016.

2. These rules shall apply to every Institution which engages in Finance Business (hereinafter referred to as the "Financial Institution") to which the provisions of the Financial Transactions Reporting Act, No.6 of 2006 (hereinafter referred to as "the Act") apply.

3. Every Financial Institution shall take the measures specified in these rules for the purpose of identifying, assessing and managing money laundering and terrorist financing risks posed by its customers, by conducting ongoing customer due diligence (hereinafter referred to as "CDD") based on the "risk based approach."

PART I

MONEY LAUNDERING AND TERRORIST FINANCING RISK MANAGEMENT

For all Financial Institutions

4. The intensity and extensiveness of risk management functions shall be in compliance with the "risk based approach" and be proportionate to the nature, scale and complexity of the Financial Institution's activities and money laundering and terrorist financing risk profile.

5. Every Financial Institution shall take appropriate steps to identify, assess and manage its money laundering and terrorist financing risks in relation to its customers, countries or geographical areas, products, services, transactions and delivery channels.

6. Every Financial Institution shall conduct the following processes in assessing money laundering and terrorist financing risks :-

(i) documenting their risk assessments and findings ;

(ii) considering all relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;

(iii) keeping the assessment up-to-date through a periodic review; and

(iv) having appropriate mechanisms to provide risk assessment information to the supervisory authority.

7. Every Financial Institution shall have proper risk control and mitigation measures including the following:-

(i) have internal policies, controls and procedures to manage and mitigate money laundering and terrorist financing risks that have been identified;

(ii) monitor the implementation of those policies, controls, procedures and enhance them if necessary; and

(iii) take appropriate measures to manage and mitigate the risks, based on the risk based approach.

8. Every Financial Institution shall conduct risk profiling on its customers considering the following :-

(i) risk level according to customer category *(ex:* different types of customers such as resident or non-resident, occasional or one-off, legal persons, politically exposed persons and customers engaged in different types of occupations);

(ii) geographical location of business or country of origin of the customer;

(iii) products, services, transactions or delivery channels of the customer *(ex:* cash-based, face-to-face or non-face-to-face, cross-border); and

(iv) any other information regarding the customer.

9. The risk control and mitigation measures implemented by every Financial Institution shall be commensurate with the risk level of a particular customer as identified based on risk profiling.

10. Upon the initial acceptance of a customer, every Financial Institution shall regularly review and update, the customer's risk profile based on his level of money laundering and terrorist financing risk.

11. A Financial Institution's money laundering and terrorist financing risk management shall be affiliated and integrated with the overall risk management relating to the Financial Institution.

12. Every Financial Institution shall provide a timely report of its risk assessment, Financial Institution's money laundering and terrorist financing risk profile and the effectiveness, of risk control and mitigition measures to, its Board of Directors. The frequency of reporting shall be commensurate with the level of risks involved and the operating environment thereof.

13. The report referred to in Rule 12 shall include the following :-

(a) results of monitoring activities carried out by the Financial Institution for combating money laundering or terrorist financing risks *(ex:* level of the Financial Institution's exposure to money laundering, and terrorist financing risk, break-down of money laundering and terrorist financing risk exposures based on key activities or customer segments, trends of suspicious transactions reports and threshold reports in terms of the Act, judicial pronouncements and freezing actions under the United Nations Security Council Resolutions);

(b) details of recent significant risks involved in either internally or externally, the *modus operandi* and its impact or potential impact on the Financial Institution; and

(c) recent developments in written laws on anti-money laundering or suppression of terrorist financing and its implications for the Financial Institution.

Internal Controls, Policies, Compliance, Audit and Training

14. (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 and suppression of terrorist financing.

(2) The detailed procedures and controls shall be developed by each Financial Institution in compliance with such policy.

15. Such policies, procedures and controls shall include, risk assessment procedures, CDD measures, manner of record retention, handling correspondent banking services, handling wire transfers, the detection and internal reporting procedure of unusual and suspicious transactions and the obligation to report suspicious transactions to the Financial Intelligence Unit.

16. Every Financial Institution shall in formulating policies, procedures and controls, take into consideration, money laundering and terrorist financing risks that may arise from the use of new or developing technologies, especially those having features of anonymity or inconsistency with the basic principles of CDD measures.

17. Every Financial Institution shall-

(*a*) appoint a senior management level officer as the compliance officer who shall be responsible for ensuring the Financial Institution's compliance with the requirements of the Act and these rules;

(*b*) ensure that the compliance officer or any other person authorized to assist him or act on behalf of him , has prompt access to all customer records and other relevant information which may be required to discharge their functions;

(*c*) develop and implement a comprehensive employee due diligence and screening procedure to be carried out at the time of appointing or hiring of all employees whether permanent, contractual or outsourced;

(*d*) frequently design and implement suitable training programmes for relevant employees including Board of Directors, in order to effectively implement the regulatory requirements and internal policies and procedures relating to money laundering and terrorist financing risk management. (The training shall enable employees to understand new developments of money laundering and terrorist financing techniques, methods and trends and their responsibilities relating to the combating of money laundering and terrorist financing risks. Particularly, requirements relating to CDD and identifying out-of pattern or unusual transactions which need to be vigilant of, and eligible to be reported as suspicious transactions); and

(*e*) maintain an independent audit function in compliance with the Code of Corporate Governance issued ,by the respective regulatory authorities that is adequately resourced and able to regularly assess the effectiveness of the Financial Institution's internal policies, procedures and controls and, its compliance with regulatory requirements.

18. For the Purpose of paragraph (e) of Rule 17, "Code of Corporate Governance" means the following:-

(*a*) Banking Act, Direction Nos. 11 and 12 of 2007 on Corporate Governance for Licensed Banks;

(*b*) Finance Companies (Corporate Governance) Direction No. 3 of 2008 for Licensed Finance Companies; and

(c) Code of Best Practice on Corporate Governance 2013 for Market Participants and Companies Listed on the Colombo Stock Exchange.

Foreign Branches and Subsidiaries

19. Financial groups shall implement group-wide programmes which shall be applicable and appropriate for all branches and majority-owned subsidiaries of the financial group with a view of combatting money laundering and terrorist financing activities and shall include the following in addition to the measures referred to in Rule 17:-

(*a*) initiate measures and procedures for sharing information required for the purposes of conducting CDD and money laundering and terrorist financing risk management;

(*b*) provide information of customers, accounts and transactions, and of audits, with group level compliance, from all branches and subsidiaries of the financial group when necessary for implementing the suppression of money laundering and terrorist financing measures; and

(*c*) maintain adequate safeguards on the confidentiality and use of information exchanged among the branches and subsidiaries of the financial group.

20. Every Financial Institution shall ensure that their foreign branches and majority-owned subsidiaries apply anti-money laundering and suppression of terrorist financing measures consistent with the domestic law requirements, where the relevant written laws of the relevant foreign country provide less stringent requirements than those provided for in the domestic law.

21. Where the foreign country does not permit the proper implementation of anti-money laundering or suppression of terrorist financing measures consistent with the domestic law requirements; every Financial Institution shall apply appropriate additional measures to manage money laundering and terrorist financing risks.

Using New Technologies

22. Every Financial Institution shall identify and assess money laundering and terrorist financing risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms and the use of new or developing technologies for both new and pre-existing products.

23. Every Financial Institution shall -

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

(*b*) take appropriate measures to manage and mitigate the risks which may arise in relation to the development of new products and new business practices; and

(*c*) not permit pre-loading of credit cards, as that may amount, *inter-alia,* to the abuse of credit cards, for money laundering and terrorist financing purposes.

Part II

CUSTOMER DUE DILIGENCE (CDD)

CDD for all Customers

24. (1) In terms of the provisions of section 2 of the Act, no Financial Institution shall open, operate or maintain any anonymous account, any account in a false name, or in the name of a fictitious person or any account that is identified by a number only (hereinafter referred to as "Numbered Account").

(2) Numbered Accounts include accounts that the ownership is transferrable without knowledge of the Financial Institution and accounts that are operated and maintained with the account holder's name omitted.

25. Every Financial Institution shall maintain accounts in such a manner that assets and liabilities of a given customer can be readily retrieved. Accordingly, no Financial Institution shall maintain accounts separately from the Institution's usual operational process, systems or procedure.

26. Every Financial Institution shall conduct the CDD measures specified in these rules, on customers conducting the transaction, when-

(*a*) entering into business relationships;

(*b*) providing money and currency changing business for transactions involving an amount exceeding rupees two hundred thousand or its equivalent in any foreign currency;

(*c*) providing wire transfer services as referred to in Rules 68 to 83;

(*d*) carrying out occasional transactions involving an amount exceeding rupees two hundred thousand or its equivalent in any foreign currency where the transaction is carried out in a single transaction or in multiple transactions that appear to be linked;

(*e*) the Financial Institution has any suspicion that such customer is involved in money laundering or terrorist financing activities, regardless of amount; or

(*f*) the Financial Institution has any doubt about the veracity or adequacy of previously obtained information.

27. (1) Every Financial Institution shall -

(*a*) idenify its customers prior entering into business relatinships ;

(*b*) obtain the information specified in the Schedule hereto, verify such information, as applicable and record the same for the purpose of identifying and initial risk profiling of customers, at minimum;

(*c*) obtain the following information for the purpose of conducting CDD, at minimum :-

(i) purpose of the account;

(ii) sources of earning;

(iii) expected monthly turnovers;

(iv) expected mode of transactions (ex; cash, cheque, etc.);

(v) expected type of counterparties (if applicable).

(2) Where any customer is rated as a customer posing a high risk, the Financial Institution shall take enhanced CDD measures for such customer, in addition to the CDD measures in sub-paragraph (c) of paragraph (1).

28. Where the customer is not a natural person, every Financial Institution shall take reasonable measures to understand the ownership and control structure of the customer and determine the natural persons who ultimately own or control the customer.

29. Where one or more natural persons are acting on behalf of a customer, every Financial Institution shall identify the natural persons who act on behalf of the customer and verify the identity of such persons. The authority of such person to act on behalf of the customer shall be verified through documentary evidence including specimen signatures of the persons so authorized.

30. Where there is a beneficial owner every Financial Institution shall obtain information to identify and take reasonable measures to verify the identity of the beneficial owner of the customer using relevant information or data obtained from a reliable source, adequate for the Financial Institution to satisfy itself that it knows who the beneficial owner is.

31. Every Financial Institution is required to verify the identity of the customer and beneficial owner before or during the course of entering into a business relationship with or conducting a transaction for an occasional customer.

Provided however; where the risk level of the customer is low according to the risk profile of the Financial Institution and verification is not possible at the point of entering into the business relationship, the Financial Institution may, subject to Rule 32 allow its customer and beneficial owner to furnish the relevant documents subsequent to entering into the business relationship and subsequently complete the verification (hereinafter referred to as “delayed verification”).

32. In any case where delayed verification is allowed the following conditions shall be satisfied:

(*a*) verification shall be completed as soon as it is reasonably practicable but not later than fourteen working days from the date of opening of the account;

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

(*c*) no suspicion of money laundering or terrorist financing risk shall be involved.

33. To mitigate the risk of delayed verification, every Financial Institution shall adopt risk management procedures relating to the conditions under which the customer may utilize the business relationship prior to verification.

34. Every Financial Institution shall take measures to manage the risk of delayed verification which may include limiting the number, type and amount of transactions that can be performed.

35. Where a Financial Institution is unable to comply with the relevant CDD measures, such Financial Institution shall, -

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

(*b*) in relation to an existing customer, terminate the business relationship, with such customer and consider making a suspicious transaction report in relation to the customer.

36. Under no circumstances shall, a Financial Institution establish a business relationship or conduct any transaction with a customer with high money laundering and terrorist financing risk, prior to verifying the identity of the customer and beneficial owner.

37. Every Financial Institution shall monitor all business relationships with a customer on an ongoing basis to ensure that the transactions are consistent with the customer's economic profile and risk profile, and where appropriate, the sources of earning.

38. (1) Every Financial Institution shall obtain information and examine the background and purpose of all complex, unusually large transactions and all unusual pattern 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 in record with a view to making such information available to the relevant competent authority when required and to make suspicious transaction report.

39. Every Financial Institution shall report transactions inconsistent with these rules to the Financial Institution's Compliance Officer for appropriate action.

40. (1) Every Financial Institution shall periodically review the adequacy of customer information obtained in respect of customers and beneficial owners and ensure that the information is kept up to date, particularly for higher risk categories of customers.

(2) The review period and procedures thereof shall be decided by each Financial Institution in its internal policy for combating money laundering and terrorist financing according to risk based approach.

41. The frequency of the ongoing CDD or enhanced ongoing CDD, shall commensurate with the level of money laundering and terrorist financing risks posed by the customer based on the risk profiles and nature of transactions.

42. Every Financial Institution shall increase the number and timing of controls applied and select patterns of transactions that need further examination, when conducting enhanced CDD.

43. Every Financial Institution shall perform such CDD measures as may be appropriate to its existing customers having, regard to its own assessment of materiality and risk but without compromise on the identity and verification requirements. In assessing the materiality and risk of an existing customer, every 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.

44. Every Financial Institution shall conduct CDD on existing customer relationships at appropriate times, taking into account whether and when CDD measures have previously been conducted and the adequacy of data obtained.

45. If an existing customer provides unsatisfactory information relating to CDD, the relationship with such customer shall be treated as a relationship posing a high risk and be subject to enhanced CDD measures.

46. Where a Financial Institution forms a suspicion of money laundering and terrorist financing risk relating to a customer and it reasonably believes that conducting the process of CDD measures would tip off the customer, it shall terminate conducting the CDD measures and proceed with the transaction and immediately file a Suspicious Transaction Report.

Occasional Customers, One-off Customers, Walk-in Customers and Third Party Customers

47. Every Financial Institution shall -

(*a*) with regard to transactions or series of linked transactions exceeding rupees two hundred thousand or its equivalent in any foreign currency conducted by occasional customers, one-off customers or walk-in customers, conduct CDD measures and obtain copies of identification documents;

(*b*) with regard to occasional customers, one-off customers or walk-in-customers who wish to purchase remittance instruments such as pay orders, drafts exceeding rupees two hundred thousand or its equivalent in any foreign currency, conduct CDD measures and obtain copies of identification documents;

(*c*) with regard to all cash deposits exceeding rupees two hundred thousand or its equivalent in any foreign currency made 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 of the third party customer:

Provided that, 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:

Provided further, if any Financial Institution has reasonable grounds to suspect that the transaction or series of linked transactions are suspicious or unusual, every Financial Institution shall, obtain such information irrespective of the amount specified above.

CDD for Legal Persons and legal arrangements

48. Every Financial Institution shall, in the case of a customer that is a legal person or legal arrangement,

(*a*) understand the nature of the customer' s business, its ownership and control structure;

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

49. In order to identify the natural person if any, who ultimately has controlling ownership interest in a legal person, a Financial Institution shall at the minimum obtain and take reasonable measures to verify the following:-

(*a*) identity of all Directors and Shareholders with equity interest of more than ten *per cent* with the requirement imposed on the legal person to inform of any change in such Directors and Shareholders;

(*b*) 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 or arrangement through independent sources;

(*c*) authorization given for any person to represent the legal person or legal arrangement either by means of Board Resolution or otherwise;

(*d*) where no natural person is identified under the preceding provisions, the identity of the relevant natural persons who hold the positions of senior management;

(*e*) when a legal person's controlling interest is vested with another legal person, Financial Institution shall identify the natural person who controls the legal person.

50. In order to identify the beneficial owners of a legal arrangement, the Financial Institution shall obtain and take reasonable measures to verify the following:-

(*a*) for Trusts, the identities of the author of the Trust, the trustees, the beneficiary or class of beneficiaries and any other natural person exercising ultimate effective control over the trust, (including those who control through the chain of control or ownership); or

(*b*) for other types of legal arrangements, the identities of persons in equivalent or similar positions.

Non-Governmental Organizations, Not-for-Profit Organizations or Charities

51. Every Financial Institution shall conduct enhanced CDD measures when entering into a relationship with a Non-Governmental Organization (hereinafter referred to as “NGO”) or a Not-for-Profit Organization (hereinafter, referred to as “NPO”) and Charities to ensure that their accounts are used for legitimate purposes and the transactions are commensurate with the declared objectives and purposes.

52. (1) Every Financial Institution shall open accounts in the name of the relevant NGO, NPO or Charity as per title given in the constituent documents thereof.

(2) The individuals who are authorized to operate the accounts and members of their governing bodies shall also be subject to enhanced CDD measures.

(3) Every Financial Institution shall ensure that the persons referred to in paragraph (2) are not affiliated with any entity or person designated as a proscribed entity or person, whether under the same name or a different name.

53. No Financial Institution shall allow personal accounts of the members of the governing bodies of a NGO, NPO or Charity to be used for charity purposes or collection of donations.

54. (1) Every Financial Institution shall review and monitor all existing relationships of a NGO, NPO or Charity to ensure that those organizations, their authorized signatories, members of their governing bodies and the beneficial owners are not linked with any entity or person designated as a proscribed entity and person, either under the same name or a different name.

(2) In case of any suspicion on similarity in names, the Financial Institution shall file a Suspicious Transaction Report or take other legal action or both.

Beneficiaries of Insurance Policies

55. 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*) for a beneficiary that is identified as specifically named natural or legal person or legal arrangement shall take the name of the person;

(*b*) for a beneficiary that is designated by characteristics or by class or by other means, shall obtain sufficient information concerning the beneficiary to satisfy the Financial Institution that it will be able to verify the identity of the beneficiary; and

(*c*) in the case of a beneficiary referred to in paragraph (*a*) and (*b*), the verification of the identity of the beneficiary shall occur at the time of appointment and payout.

56. Every Financial Institution shall include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are to be applicable. If the Financial Institution determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, it shall take 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 payout.

Customers and Financial Institutions from High Risk Countries

57. (1) Every Financial Institution shall apply the enhanced CDD measures to business relationships and transactions to customers and Financial Institutions from high risk countries.

(2) The Secretary to the Ministry of the Minister to whom the subject of Foreign Affairs has been assigned or the subject of Defence has been assigned, as the case may be, shall specify the high risk countries referred to in paragraph (1)-

(*a*) based on the Financial Action Task Force listing; or

(*b*) independently taking into account, the existence of strategic deficiencies in anti-money laundering and suppression of terrorist financing policies and not making sufficient progress in addressing those deficiencies in those countries.

(3) Upon specifying the high risk countries as specified in paragraph (2), the Financial Intelligence Unit shall publish the list of high risk countries in its official website.

(4) The type of enhanced measures applied under paragraph (1) shall be effective and correspond to the nature of risk.

58. In addition to enhanced CDD measures, every Financial Institution shall apply appropriate counter measures, as follows, for countries specified in the list of high risk countries referred to in paragraph (2) of Rule 57, corresponding to the nature of risk of listed high risk countries:-

(*a*) limiting business relationships or financial transactions with identified countries or persons located in the country concerned;

(*b*) review and amend or, if necessary terminate, correspondent banking relationships with Financial Institutions in the country concerned;

(*c*) conduct enhanced external audit, by increasing the intensity and frequency, for branches and subsidiaries of the Financial Institution or financial group, located in the country concerned; and

(*d*) conduct any other measure as may be specified by the Financial Intelligence Unit.

Politically Exposed Persons (PEPs)

59. In relation to politically exposed persons or their family members and close associates, every Financial Institution shall -

(*a*) implement appropriate internal policies, procedures and controls to determine if the customer or the beneficial owner is a politically exposed person;

(*b*) obtain approval from the Board of Directors of the Financial Institution to enter into or continue business relationship where the customer or a beneficial owner is a politically exposed person or subsequently becomes a politically exposed person;

(*c*) identify, by appropriate means, the sources of funds and wealth or beneficial ownership of funds and wealth; and

(*d*) conduct enhanced ongoing monitoring of business relationships with the politically exposed person.

60. In relation to life insurance policies of politically exposed persons, every Financial Institution shall-

(*a*) take reasonable measures to determine whether the beneficiary, beneficiaries or the beneficial owner, as the case may be, are politically exposed persons, at the time of the payout;

(*b*) where higher risks are identified, inform Senior Management before the payout of the policy proceeds, to conduct enhanced scrutiny on the whole business relationship with the policy holder, and consider whether to make a suspicious transaction report or not.

Financial Institution which relies on a Third-Party

61. Where any Financial Institution is permitted to rely on a third-party Financial Institution or designated non finance business in order to conduct CDD measures, including the identification of the customer, identification of the beneficial owner and understanding the nature of the business or initiating the business, the ultimate responsibility for CDD measures shall remain with the Financial Institution relying on the third party, which shall-

(*a*) obtain immediately the necessary information relating to CDD ;

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

(c) satisfy itself that the third party Financial Institution or designated non-finance business is regulated, supervised or monitored, and has measures to adhere to CDD and record-keeping requirements in compliance with the Act.

62. Every Financial Institution which relies on third party shall,

(a) have internal policies and procedures which enables the mitigation of anti-money laundering and terrorist financing risks to the international financial system, including those from countries that have been identified by the Financial Action Task Force as having strategic deficiencies in anti-money laundering and suppression of terrorist financing policies;

(b) have regard to information available on the level of country risk, when determining the country of a third party .

63. The provisions of Rules 61 and 62 shall apply in respect of every Financial Institution which relies on a third party that is part of the same financial group or group of companies in the following circumstances:-

(a) when applying CDD and record-keeping requirements and implementing anti-money laundering or suppression of terrorist financing programmes, in accordance with the relevant written laws;

(b) when conducting supervision by the Financial Intelligence Unit or any relevant authority, of the implementation of CDD and record-keeping requirements and anti-money laundering or suppression of terrorist financing programmes, at group level; and

(c) when any risk arising due to a third party located in a high risk country referred to in Rule 57, is solely mitigated by the group' s anti-money laundering or suppression of terrorist financing internal policies.

PART III

CORRESPONDENT BANKING

64. (1) Every Financial Institution providing correspond banking services to respondent banks (hereinafter referred to as the "correspondent bank") shall take necessary measures to ensure that the risk of money laundering and terrorist financing through the accounts of the respondent banks *(ex.* being used by shell banks) are duly managed.

(2) Accordingly, every correspondent bank shall assess the suitability of the respondent bank by taking the following measures;

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

(i) internal policy of the respondent bank on anti- money laundering and suppression of terrorist financing;

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

(iii) core business activities;

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

(v) money laundering prevention and detection measures;

(vi) the purpose of the account or service;

(vii) identity of any third party that will use the correspondent banking services *(i.e.* in case of payable-through accounts);

(viii) the level of the regulation and supervision of banks in the country of the respondent bank.

(b) determine from publicly available sources, the reputation of the respondent bank, and as far as practicable, the quality of supervision over the respondent bank, including facts as to whether it has been subject to money laundering or terrorist financing investigation or regulatory action;

(c) assess the respondent bank's anti-money laundering and suppression of terrorist financing systems and ascertain whether they are adequate and effective, having regard to the anti- money laundering and suppression of terrorism financing measures of the country or jurisdiction in which the respondent bank operates;

(d) clearly understand and record the respective anti-money laundering and suppression of terrorist financing responsibilities of each bank; and

(e) obtain approval of the Board of Directors of the respondent bank, before entering into new correspondent banking relationships.

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

(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.

66. Every correspondent bank shall apply enhanced CDD measures when entering into or continuing correspondent banking relationship with banks or Financial Institutions which are located in high risk countries, referred to in Rule 57.

67. (1) No correspondent bank shall enter into or continue correspondent banking relationship with a shell bank.

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

PART IV

WIRE TRANSFERS

68. Every Financial Institution shall in processing wire transfers, take freezing action and comply with prohibitions on conducting transactions with designated persons and entities, as per obligations set out in the United Nations Regulation No.1 of 2012 published in *Gazette* Extraordinary No. *1758/19* dated May 15, 2012 and United Nations Regulation No. 2 of 2012 published in *Gazette* Extraordinary No.*1760/40* dated May 31, 2012, relating to the prevention and suppression of terrorism and terrorist financing, inclusive of United Nations Security Council Resolutions 1267 and 1373 and any successor resolutions thereto.

69. Every Financial Institution shall preserve Society for Worldwide Interbank Financial Telecommunication (SWIFT) messages that accompany inward remittances for a period of six years from the date of transaction.

Ordering Financial Institutions

70. Every Ordering Financial Institution shall ensure that all cross-border wire transfers having a value more than or equal to rupees one hundred thousand or its equivalent in any foreign currency to be always accompanied with the following :-

(a) originator information :-

(i) name of the originator;

(ii) originating 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) originator's address, national identity card number or any other customer identification number as applicable;

(b) beneficiary information :-

(i) name of the beneficiary; and
(ii) the beneficiary account number where such an account is used to process the transaction or in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

71. Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file shall contain required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country and shall include the originator's account number or unique transaction reference number.

72. Every Ordering Financial Institution shall verify the information pertaining to its customer where there is a suspicion of money laundering and terrorist financing risk.

73. In the case of domestic wire transfers, the Ordering Financial Institution shall ensure that the information accompanying the wire transfer includes originator information as indicated for cross-border wire transfers unless such information can be made available to the Beneficiary Financial Institution and appropriate authorities by other means.

74. (1) In the case 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 make the information available as soon as practicable after receiving the request either from the Beneficiary Financial Institution or from the appropriate authority.

75. Every Ordering Financial Institution shall maintain all originator and beneficiary information collected, in accordance with the Act.

76. If any Ordering Financial Institution fails to comply with the requirements specified in Rules 70 to 75 (both inclusive) in respect of a wire transfer, such Financial Institution shall not proceed with the wire transfer unless directed to do so by the Financial Intelligence Unit and shall consider reporting the relevant transaction as a suspicious transaction to the Financial Intelligence Unit.

Intermediary Financial Institution

77. Every Financial Institution which is involved in wire transfers as an Intermediary Financial Institution shall ensure that for cross-border wire transfers, all originator and beneficiary information that accompanies a wire transfer is retained with the wire transfer message.

78. 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.

79. Every Intermediary Financial Institution shall take reasonable measures, which are consistent with straight-through processing to identify cross-border wire transfers that lack the required originator information or required beneficiary information.

80. Every Intermediary Financial Institution shall have risk-based internal policies and procedures for determining-

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

Beneficiary Financial Institution

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

82. For cross-border wire transfers of rupees one hundred thousand or above or its equivalent in any foreign currency, a Beneficiary Financial Institution shall verify the identity of the beneficiary, and maintain the information in accordance with the Act if the identity has not been previously verified.

83. 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; and
(b) what is the appropriate follow up action.

Money or Value Transfer Service Providers

84. Every provider of Money or Value Transfer Service (hereinafter referred to as "MVTS") shall maintain a current list of its agents in all countries in which the MVTS provider and its agents operate.

85. Every MVTS provider that uses agents shall include them in its internal policy on anti-money laundering or suppression of terrorist financing and monitor them in compliance with that policy.

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

87. 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 the ordering customer and the beneficiary customer, in order to determine whether a suspicious transaction report needs to be filed; and

(b) file a suspicious transaction report with the Financial Intelligence Unit, on identifying a suspicious wire transfer.

88. (l) Every Financial Institution shall follow special precautionary measures to make a distinction between formal money transmission services and other alternative money or value transfer systems *(ex:* hundi, hawala etc.) through which funds or value are moved from one geographic location to another, through informal and unsupervised networks or mechanisms.

(2) The Financial Institution shall take reasonable measures to ascertain the sources of funds involving any such alternative money or value transfer system and file a suspicious transaction report with the Financial Intelligence Unit.

Part V

RECORD KEEPING

89. Every Financial Institution shall maintain all records of transactions, both domestic and international, including the results of any analysis undertaken, such as inquiries to establish the background and purpose of complex, unusually large transactions for a minimum period of six years from completion of such transactions.

90. The records shall be sufficient to permit reconstruction of individual transactions including the nature and date of the transactions, the type and amount of currency involved and the type and identifying number of any account involved in the transactions so as to be produced in a court of law, when 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.

91. The records of identification data obtained through CDD process such as copies of identification documents account opening forms, know your customer related documents, verification documents and other documents along with records of account files and business correspondence, shall be maintained for a minimum period of six years commencing from the date on which the busines relationship was fulfilled or the occasional transaction was effected.

92. The records shall be maintained up-to-date and be kept in original or copies with the Financial Institution's attestation.

93. Every Financial Institution shall retain the above records for a longer period where transactions customers or accounts are involved in litigation or required to be produced in a court of law or before any other appropriate authority.

94. (l) Every Financial Institution shall ensure that all CDD information and transaction records are available immediately to relevant domestic authority and Financial Intelligence Unit.

(2) For the purposes of this rule relevant domestic authority means -

(*a*) Any public authority (including a supervisory authority established as independent non-governmental authority with statutory powers) with designated responsibilities for prevention of money laundering and suppression of terrorist financing;

(*b*) Any authority that performs the function of investigating and prosecuting money laundering and terrorist financing associated offences and seizing or freezing and confiscating assets relating to such offences; and

(*c*) Any authority receiving reports on cross-border transportation of currency.

PART VI

MISCELLANEOUS

95. Every Financial Institution shall verify whether any prospective customer or beneficiary appears on any suspected terrorist list or alert list issued in compliance with the United Nations Regulations No. 1 of 2012 published in *Gazette* Extraordinary No. 1758/19 dated May 15, 2012 and United Nations Regulations No. 2 of 2012 published in *Gazette Extraordinary* No. 1760/40 dated May 31, 2012, relating to the prevention and suppression of terrorism and terrorist financing, inclusive of United Nations Security Council Resolutions 1267 and 1373 and any successor resolutions thereto.

96. In the case of a prospective customer whose permanent 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 discourage or turn down the request to open the account and shall request the prospective customer to open the account at the closest branch to the customer's residence or business, unless an acceptable and a valid reason is given to keep in record.

97. Where two or more accounts are opened in the same Financial Institution by one customer, the Financial Institution shall record the specific purpose for which such accounts are opened, in order to enable ongoing CDD of all accounts.

98. The Licensed Banks and Registered Finance Companies (Know Your Customer (KYC) and Customer Due Diligence (CDD)) Rules, No. 1 of 2011 published in *Gazette* Extraordinary No. 1699/10 of March 28, 2011 are hereby rescinded without prejudice to anything previously done thereunder.

99. In these Rules —

"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 institution directly or through an intermediary institution and makes the funds available to the beneficiary customer;

"beneficial owner" means a natural person who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted and includes the person who exercises ultimate effective control over a person or a legal arrangement;

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

"customer" in relation to a transaction or an account includes-

(a) the person in whose name a transaction or an account is arranged, opened or undertaken;
(b) a signatory to a transaction or an account;
(c) any person to whom a transaction has been assigned or transferred;
(d) any person who is authorized to conduct a transaction; or
(e) such other person as may be prescribed;

"correspondent banking" means provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank) pincluding cash management *(ex:* large international banks frequently act as correspondent banks for large number of other banks around the world by providing 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);

"close associate" includes -

(a) a natural person having joint beneficial ownership of legal entities and legal arrangements, or any other close business relationship; 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;

"controlling interest" means an interest acquired by providing more than ten *percent* of the capital of a Financial Institution;

"Company Act" means the Companies Act, No. 7 of 2007 ;

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

"Financial Action Task Force" means an independent inter-governmental body that develops land promotes policies to protect the global financial system against money laundering, terrorist financing and the financing for proliferation of weapons of mass destruction;

"financial group" means a 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 suppression of terrorist financing policies and procedures, together with branches and subsidiaries that are subject thereto;

"finance company" means a company licensed under the Finance Business Act, No. 42 of 2011;

"immediate family member" includes the spouse, children and their spouses or partners, parents, siblings and their spouses and grandchildren and their spouses;

"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 institution, or another intermediary institution;

"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;

“legal arrangment” includes an express trust, a fiduciary account or a nominee ;

"licensed bank" means any commercial bank and specialized bank, licensed under the Banking Act, No. 30 of 1988;

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

"MVTS" means financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message transfer or through a clearing network to which the relevant financial service provider belongs. Transactions performed by such service may involve one or more intermediary transactions and a final payment to a third party and may indude any new payment methods ;

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

"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;

"person" means a natural or legal person and includes a body of persons whether incorporated or unincorporated and a branch incorporated or established outside Sri Lanka;

"politically exposed person" means an individual who is entrusted with prominent public functions either domestically or by a foreign country, or in an international organization and includes a Head of a State or a Government, a politician, a senior government officer, judicial officer or military officer, a senior executive of a State owned Corporation, Government or autonomous body but does not include middle rank or junior rank individuals;

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

"risk based approach" in relation to the application of CDD measures to manage and mitigate money laundering and terrorist financing risks, means the use of simplified CDD measures in the case of customers with lower risk levels and the use of enhanced CDD measures in the case of customers with higher risk levels;

“Suspicious Transaction Report” means a report of a suspicious transaction or attempted transaction as per section 7 of the Act ;

"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;

"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.

SCHEDULE

(Rule 27)

(1) **Individual Customers :**

(a) The follwing information shall be obtained :-

(a1) In the case of all customers -

(i) Full name as appearing in the identification document;

(ii) Official personal identification or any other identification document that bears a photograph of the customer (*ex:* national identity card, valid passport, or valid driving licence) ;

(iii) Permanent address as appearing on the identification document. If 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 except for State owned enterprises. In the case of 'C/o', property owner's consent and other relevant address verification documents are required to be obtained;

(iv) Telephone number, facsimile number, and e-mail address (if available);

(v) Date of Birth;

(vi) Nationality

(vii) Occupation, business, public position held and the name of the employer and geographical areas involved (if available);

(viii) Purpose for which the account is opened;

(ix) Expected turnover/volume of business ;

(x) Expected mode of transactions ;

(xi) Satisfactory reference, as applicable; and

(a 2) In the case of non-resident customers -

(i) The reason for opening the account in Sri Lanka ;

(ii) Name, address and the copy of passport of the person or persons authorized to give instructions;

(b) The following documents shall be obtained (each copy shall be verified against the original)

(i) Copy of identification document;

(ii) Copy of address verification document;

(iii) Copy of the valid visa/permit in the case of accounts for non-national customers.

(2) **Proprietorship/Partnership Accounts :**

(a) The following information shall be obtained :-

(i) Full names of the partners or proprietors as appearing in the business registration document;
(ii) Nature of the business;
(iii) Registered address or the principal place of business;
(iv) Identification details of the proprietor/partners as in the case of individual accounts;
(v) Contact telephone, fax numbers;
(vi) Income Tax file number;
(vii) The extent of the ownership controls;
(viii) Other connected business interests;

(b) The following documents shall be obtained (each copy shall be verified against the original) :-

(i) Copy of the business registration document;
(ii) Proprietors' information / Partnership Deed;
(iii) Copy of identification and address verification documents.

(3) Corporations/Limited Liability Company :

(a) The follwing information shall be obtained :-

(i) Registered name and the Business Registration Number of the institution;
(ii) Nature and purpose of business;
(iii) Registered address of the principal place of business;
(iv) Mailing address, if any;
(v) Telephone/Fax/E-mail ;
(vi) Income Tax file number;
(vii) Bank references (if applicable);
(viii) Identification of all Directors as in the case of individual customers;
(ix) List of major shareholders with equity interest of more than ten *percent;*
(x) Lists of subsidiaries and affiliates;
(xi) Details of names of the signatories;

Note : In the case of companies listed on the Stock Exchange of Sri Lanka licensed under the Securities and Exchange Commission of Sri Lanka Act, No. 36 of 1987 or any other stock exchange subject to disclosure requirements ensuring adequate transparency of the beneficial ownership, the Financial Institution may use the information available from reliable sources to identify the Directors and major Shareholders;

(b) The following documents shall be obtained (each copy shall be verified against the original):-

(i) Copy of the Certificate of Incorporation ;
(ii) Copy of Form 40 (Registration of an existing company) or Form l (Registration of a company) under the Companies Act and Articles of Association;
(iii) Board Resolution authorizing the opening of the account;
(iv) Copy of Form 20 (Change of Directors/Secretary and Particulars of Directors/Secretary) under the Companies Act;
(v) Copy of Form 44 (Full address of the registered or principal office of a company incorporated outside Sri Lanka and its principal place of business established in Sri Lanka) under the Companies Act;
(vi) Copy of Form 45(List and particulars of the Directors of a company incorporated outside Sri Lanka with a place of business established in Sri Lanka) under the Companies Act;
(vii) Copy of the Board of Investment Agreement if a Board of Investment approved company;

(viii) Copy of the Export Development Board (EDB) approved letter if EDB approved company;

(ix) Copy of the certificate to commence business if a public quoted company;

(x) Name of the person or persons authorized to give instructions for transactions with a copy of the Power of Attorney or Board Resolution, as the case may be;

(xi) Latest audited accounts if available.

Note: The above documents shall apply to a company registered abroad as well. The non-documentary methods in the absence of the above documents would entail a search at the Credit Information Bureau (CRIB), bank references, site visits and visiting the business website of the customer.

(4) Clubs, Societies, Charities, Associations and Non-Governmental Organizations:

(*a*) The following information shall be obtained:-

(i) Registered Name and the Registration Number of the institution;

(ii) Registered address as appearing in the Charter, Constitution etc.;

(iii) Identification of at leas 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 as in the case of individual accounts;

(iv) Committee or Board Resolution authorizing the account opening;

(v) The source and level of income/funding;

(vi) Other connected institutions/associates/organizations;

(vii) Telephone/Facsimile numbers/E-mail address.

(*b*) The following documents shall be obtained and be verified against the original:-

(i) Copy of the registration document/constitution charter etc.;

(ii) Board Resolution authorizing the account opening;

(iii) Name of the persons authorized to give instructions for transactions with a copy of the Power of Attorney or Board/Committee Resolution;

(5) Trust nominees and Fiduciary accounts :

(a) The following information shall be obtained: -

(i) Identification of all trustees, settlers/grantors and beneficiaries in case of trusts as in the case of individual accounts;

(ii) Whether the customer is acting as a 'front' or acting as a trustee, nominee, or other intermediary;

(b) The following documents shall be obtained (each copy should be verified against the original) :-

(i) Copy of the Trust Deed, as applicable ;

(ii) Particulars of all individuals.

(6) Stocks and Securities Sector specific requirements :-

(*a*) The following information shall be obtained from the Funds approved by the Securities and Exchange Commission of Sri Lanka:-

(i) Name of the Fund;

(ii) Purpose of the Fund;

(iii) Place of establishment of the Fund;
(iv) Details (name, address, description etc.,) of the Trustee/Manager of the Fund;
(v) If the Trustee/Manager is a company, date of incorporation, place of incorporation, registered addresss of such trustee/Manager;
(vi) Copies of the documents relating to the establishment and management of the fund (*ex:* Prospectus/Trust Deed/Management Agreement/Bankers Agreement /Auditors Agreement);
(vii) Copy of the letter of Approval of the Fund issued by the Supervisory Authority of the relevant country;
(viii) Copy/copies of the relevant Custody Agreement/s;
(ix) Details of beneficiaries.

(*b*) Certification requirement :-

All supporting documents to be submitted to Central Depository System shall be certified, attested or authenticated by the persons specified in (A) or (B) below for the purpose of validating the applicant:-

(A) For Non- resident applicants :-

(i) By the Company Registrar or similar authority;
(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, an Attorney -at- Law, a Notary Public 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;

(B) For resident applicants :-

(i) By the Registrar of Companies or the Company Secretary (applicable in respect of Corporate Bodies);
(ii) By an Attorney- at- Law or a Notary Public;
(iii) By a Broker; or
(iv) By the Custodian Bank.

Note: (I) The person certifying shall place the signature, full name, address, contact telephone number and the official seal (Not applicable for Brokers, Custodian Banks and Global Custodians).

(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 company shall be submitted together with a declaration from the Global Custodian that a custody arrangement or agreement exists between the Global Custodian and the Beneficiary.

02 - 346

PRINTED AT THE DEPARTMENT OF GOVERNMENT PRINTING, SRI LANKA.