The Republic of the Union of Myanmar

Central Bank of Myanmar

Directive No. (18/2019)

(Directive for the CDD Measures)

4th Waning Day of Tazaungmone 1381 ME

November 15, 2019

Introduction

1. In exercising the power set out in the Section 69(c) of the Anti-Money Laundering Law and Section 40 of the Central Bank of Myanmar Law, the Central Bank of Myanmar issues the Directive on Customer Due Diligence related to the Anti-money Laundering and Counter Financing of Terrorism to the banks licensed and supervised by the CBM.

Background

2. All Banks and Financial institutions are required to develop effective frameworks and practices to manage their money laundering/terrorist financing (ML/TF) risks. It is important that banks and financial institutions licensed to operate in Myanmar have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate customer due diligence on new and existing customers is a key part of these controls. Without this, banks and financial institutions can become subject to reputational, operational, legal and concentration risks, which can result in significant financial cost.

Definitions

3. Unless the subject or context otherwise requires, in this Directive:
   (a) "Law" means the Anti-money Laundering Law enacted on March 14, 2014.
   (b) "Bank" means Banks as defined in Section 2(c) of the Financial Institutions Law.
   (c) "CDD" means Customer Due Diligence as defined in section 3(u) of the Law and as described in Article 9 to 39 of this Directive.
   (d) "Business relationship" means any business, professional or commercial relationship connected with the professional activities of a bank and which is expected to have an element of duration.
   (e) "Financial Intelligence Unit (FIU)" means the Financial Intelligence Unit established by the Central Body pursuant to Section 9 of the Law.
   (f) "PEP" means a politically exposed person as defined in Section 3(l) and 3(m) of the Law.
   (g) "FATF" means the Financial Actions Task Force.
   (h) "Ordering bank" means the bank or financial institution which requests the transfer of funds on behalf of a natural or legal person.

(i) "Correspondent banking" means the provision by one bank (the correspondent) to another bank (the respondent) of credit, deposit, collection, clearing or payment services.

(j) "Settlor" means a natural or legal person who transfers ownership of their assets to trustees by means of a trust deed or similar arrangement.

(k) "Trustee" should be understood as described in and consistent with Article 2 of the Hague Convention " Convention on the Law Applicable to Trusts and on their Recognition" and "the Trust Act, 1904" applicable to trusts and their recognition. Trustees may be professional (e.g. depending on the jurisdiction, a lawyer or trust company) if they are paid to act as a trustee in the course of their business, or nonprofessional (e.g. a person acting without reward on behalf of family).

(l) "Beneficial Owner" refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

(m) "Beneficiary" means;

(i) as used in Article 31 (b) of this Directive, the person or persons who are entitled to the benefit of any trusts arrangement. A beneficiary can be a natural or legal person or arrangement.

(ii) For the purposes of Policies and Procedures on Wire or Electronic Transfers of this Directive, the natural or legal person who is identified by the originator as the receiver of the requested Wire or Electronic Transfers.

(n) "Originator" means the account holder, or where there is no account, the person (natural or legal) that places the order with the bank or financial institution to perform a wire or electronic transfers.

(0) "Payable-through accounts" refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

Policies and Procedures

4. Pursuant to section 28 of the Law, banks shall adopt, develop and implement internal policies, procedures, systems, and controls to combat money laundering and terrorism financing. These internal policies, procedures, systems and controls should address the following requirements:

(a) Risk assessments of the customer as well as transactions.

(b) Identification and verification of the customer, including walk-in/occasional customers, beneficial owners.

(c) Application of customer due diligence measures to customers

(d) Exercising ongoing customer due diligence measures in relation to business relations and transactions.

(e) Application of enhanced customer due diligence measures to high risk customers, including politically exposed persons.

(f) Maintaining records and information of customers and transactions.

(g) Monitoring transactions set out in section 21 of the Law.

(h) Reporting to the Financial Intelligence Unit of transactions as set out in section 32 and 34 of the Law.

(i) Ensuring that internal policies, procedures, systems and controls are subject to independent audit function and review.

(j) The appointment of a compliance officer at senior management level to ensure compliance with the provisions of the Law, Rules issued under the Law and this Directive.

(k) Ensuring high standards of integrity while recruiting employees.

(l) Providing an on-going training program to all new and existing employees, directors, board members, and executive or management staff.

(m) Other arrangements as prescribed by the CBM and competent regulatory authorities.

5. Bank, in developing and implementing the internal policies, procedures, systems and controls, shall –

(a) do so in a manner consistent with the bank's size, and nature and scope of operations

(b) apply the measures to all domestic and foreign branches and majority-owned subsidiaries of the bank.

(c) review and update internal policies, procedures, systems and controls on a regular basis.

(d) submit information on its internal policies, procedures, systems and controls to the CBM when requested to do so.

Conducting risk assessments

6. (a) Bank shall develop and adopt measures to identify, assess, monitor, manage and mitigate money laundering and terrorism financing risks including the risks associated with new products or technologies.

(b) The risk assessment and any underlying information shall be documented in writing, be kept up-to-date and readily available for the CBM to review at its request.

(c) In assessing their money laundering and terrorism financing risks under Sub-Article (a), banks should give consideration to the following factors such as:

(1) Customer risk;

(2) Country or Geographic region risk; (i.e. countries or geographic areas in which customers operate or the place of origination or destination of transactions);

(3) Products and services risks; (i.e. the risks that arise from the products and services offered) and

(4) Delivery channel risk: (i.e. the risks that arise from the channels used to deliver products and services).

7. In respect of the risk factors set out in Article 6(c), high risk situations where bank should apply enhanced CDD measures include but are not limited to the following:

(a) Customer risk factors:

(1) The business relationship is conducted in unusual circumstances. Non-resident customers.

(2) Legal persons or arrangements that manage the assets of third parties.

(3) Companies that have nominee shareholders or shares in bearer form.

(4) Activities that are cash-intensive or susceptible to money laundering or terrorism financing.

(5) The ownership structure of the legal person appears unusual or excessively complex with no visible economic or lawful purpose given the nature of the company's business.

(6) Business relationships conducted in or with countries as identified by the Financial Intelligence Unit under section 31(a) of the Law.

(7) Politically exposed persons ("PEP") or customers linked to a PEP.

(8) High net worth customers, or customers whose source of income or assets is unclear.

(9) Businesses/activities identified by the FIU, the Central Body, the CBM or the FATF as of higher money laundering or financing of terrorism risk.

(b) Country or geographic risk factors:

(1) Countries classified by credible sources, such as mutual evaluation reports or published follow-up reports, as not having adequate AML/CFT systems.

(2) Countries identified by the FATF, Central Body, FIU or CBM as high risk.

(3) Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.

(4) Countries classified by credible sources as having significant levels of corruption or other criminal activity.

(5) Countries or geographic areas classified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

(c) Product, service, transaction or delivery channel risk factors:

(1) Private banking.

(2) Anonymous transactions (which may include cash)

(3) Accounts opened, business relationships or transactions conducted with customers that are not physically present for the purpose of identification.
(4) Payment received from unknown or un-associated third parties.
(5) Complex trade financing products.

8. Bank shall adopt and apply the following risks mitigation measures based on the risk assessment in line with Articles 6 and 7 of this Directive;

(a) Obtain additional information on the customer, beneficial owner, beneficiary and transaction.
(b) Develop a risk profile on customers and transactions should be established and documented based on the following:
(1) the purpose of an account or relationship,
(2) the customer's anticipated business with the bank,
(3) the source of funds and source of wealth of the customer,
(4) knowledge of the customer and beneficial owner.
(5) Apply enhanced customer due diligence to high risk customers.
(6) Update more regularly the information on all customers.
(7) Monitor the amount, type and frequency of customer transactions.
(8) Adopt other measures as may be prescribed by the CBM, the Central Body or the FIU.

Customer Identification Requirements

9. Bank shall not maintain or open an account or business relationship of unknown identity or in fictitious names.

10. Bank shall ensure that they know the true identity of their customers, including beneficial owners as set out in section 19 of the Law and Articles 9, 10 and 11 of this Directive.

11. In addition to customer due diligence measures set out Section 19(d) of the Law, banks:

(a) regarding natural persons, must verify the identity of their customers using reliable, independent source documents, data, or information as outlined in **Schedule** of this Directive.
(b) regarding legal persons or legal arrangements, must obtain and verify the information required using reliable, independent source documents, data, or information as outlined in **Schedule** of this Directive.

12. Where a bank is unable to comply with the requirements of Articles 9, 10 and 11 of this Directive, it should terminate the relationship and consider submitting a suspicious transaction report to the FIU.

13. Legible file copies should be taken of the relevant identification documents for all customers both natural and legal persons.

Delayed Customer Identification Verification

14. Bank may engage in the business relationship with the customer prior to the completion of the customer verification process outlined in Articles 9, 10 and 11 of this Directive provided all of the following circumstances are met:

(a) when the verification occurs as soon as reasonably practicable;
(b) when it is essential not to interrupt the normal conduct of business;
(c) when the ML and TF risks are effectively managed.

15. Bank should include in their risk management procedures concerning delayed customer verification a set of minimum requirements such as a limitation on the number, types or amount of transactions that can be performed by the customer.

Enhanced and Simplified Customer Due Diligence

16. Bank:

(a) shall apply enhanced customer due diligence procedures to customers or transactions that have been identified as high risk. This risk assessment should be kept up to date.
(b) may apply simplified customer due diligence procedures to customers that have been identified as low risk through a documented risk assessment. This risk assessment should be kept up to date.

Enhanced CDD for occasional transactions

17. Bank shall require to undertake enhanced CDD measures when carrying out occasional transactions of a customer who has no established relationship with the bank if the transaction amount is equal to or above the threshold of Kyat or any other currencies equivalent of (USD 15,000), including situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

Enhanced CDD for Higher Risk Customers

18. The enhanced customer due diligence to be applied by bank for higher risk customers should include:

(a) Examining, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose.
(b) Increasing the degree and nature of monitoring of the business relationship regarding the transactions or performance prescribed in Sub-Article (a), in

order to determine whether those transactions or activities appear unusual or suspicious.

(c) Obtaining additional information on the customer (e.g. occupation, volume of assets,), and updating more regularly the identification data of customer and beneficial owner.

(d) Obtaining additional information on the intended nature of the business relationship.

(e) Obtaining information on the source of funds or source of assets of the customer.

(f) Obtaining information on the reasons for intended or performed transactions.

(g) Obtaining the approval of senior management to commence or continue the business relationship.

(h) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

(i) creating a customer profile or monitoring in place to be able to support identification of unusual transactions for higher risk clients including PEPs.

(j) Carrying out customer due diligence measures on the first transaction conducted through the account opened with the customer's name.

19. Bank should apply the enhanced customer due diligence measures to higher risk customers at each stage of the customer due diligence process and on an on-going basis.

20. Enhanced customer due diligence measures for business relationships with customers not physically present for the purpose of identification should include the following:

(a) certification of documents in line with relevant Laws and this Directives;

(b) requesting additional documents and development of independent verification measures and/or contact with the customer.

Politically Exposed Persons

21. Bank shall establish appropriate risk-management systems to determine whether a customer or beneficial owner is a politically exposed person and apply the additional customer due diligence measures set out in section 22 of the Law.

22. Measures for determining who is a politically exposed person, whether a customer or beneficial owner, should include:

(a) seeking relevant information from the customer;

(b) referring to information about the customer;

(c) referring to commercial electronic databases of PEPs; and

(d) taking reasonable measures to determine whether the beneficiary(ies) of a life insurance policy and/or the beneficial owner of the beneficiary are politically exposed persons. This should occur, at the latest, at the time of the payout.

23. Where higher risks are identified, in addition to performing the customer due diligence measures specified in Article 22(d) of the Directive, bank shall:

(a) seek approval of senior management before the payout proceeds; and

(b) conduct enhanced scrutiny of the business relationship with the policyholder and consider submitting a suspicious transaction report to the FIU.

Simplified Customer Due Diligence for Low Risk Customers

24. The simplified CDD measures should be commensurate with the risk factors as mentioned in this Directive and could include, but are not limited to the following:

(a) Reducing the frequency of customer identification updates.

(b) Reducing the degree of on-going monitoring and scrutinizing transactions.

(c) Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship.

25. Bank shall not apply simplified customer due diligence measures whenever there is a suspicion of money laundering or terrorism financing or when the customer has a business relationship with or in countries not applying sufficient measures to prevent money laundering and terrorist financing or those who have been listed by the FATF or identified by the FIU as being high risk or where higher risk scenarios apply as identified by the bank.

Determination of Beneficial Owner

26. If a bank determines that the customer is acting on behalf of one or more beneficial owners, they should verify the identity of the beneficial owner by using relevant information or data obtained from a reliable source such that the bank is satisfied that it knows the identity of the beneficial owner.

27. The information to be obtained on a beneficial owner under Article 26 above should be consistent with the requirements outlined in Schedule of this Directive.

28. The requirement prescribed in Articles 26 and 27 of this Directive includes accounts opened by lawyers or law offices on behalf of their clients and by trustees. Bank should apply customer due diligence measures on the beneficial owner in these cases.

29. If a customer is a company listed on a stock exchange, a bank is not required to identify and verify the identity of any shareholder or beneficial owner of the company provided that the company is subject to adequate disclosure requirements to ensure transparency of beneficial ownership. In this case, the bank should only obtain customer identification documents on the company itself and obtain the relevant identification data from public register or if not available from a public register, the reporting organization shall obtain the information from the customer.

30. Relating to customers that are legal persons or arrangements, bank should take adequate measures to understand their ownership and control structure.

31. (a) With respect to such legal persons or arrangement, identification should be made of each natural person that:
    (1) Owns or controls directly or indirectly more than 20 percent of the legal entity or exercises control of the legal person or arrangement through other means;
    (2) Is responsible for the management of the legal entity.

(b) With respect to legal arrangements, identification should be made of the Settlor, trustee, protector, beneficiary or of persons in similar positions and any other person exercising ultimate effective control including through a chain of control/ownership.

32. Bank shall obtain information (including the following but not limited to) of the trustee before it establishes a business relationship or carries out an occasional transaction equal to or above the threshold set out in Article 17 of the Directive;

(a) A trustee shall disclose its status to the bank.
(b) A Trustee shall provide the banks with information on the beneficial ownership and the assets of the trust to be held or managed under the terms of the business relationship.

Maintenance of Customer Information

33. Bank shall gather and maintain customer and beneficial owner(s) information throughout the course of the business relationship. Documents, data, or information and business correspondence collected under the customer due diligence process should be kept up to date and relevant by undertaking reviews of existing records at appropriate times as determined by the bank when:

(a) A significant transaction is to take place;
(b) There is a material change in the way the account is operated;
(c) Information held on the customer is insufficient to enable the bank to understand the nature of the banking relationship or transactions being conducted.

Ongoing Monitoring of Customer Transactions

34. Bank should adopt procedures, such as computerized automated systems, to monitor on an ongoing basis customer transactions and the relationship with the customer as required by **section 20** of the Law.

35. As required by section 20 of the Law, the monitoring undertaken by bank shall include the scrutiny of customer transactions to ensure that they are being conducted according to the bank's knowledge of the customer, the customer's commercial activities, the customer risk profile and, where necessary, the source of funds and wealth, and shall include predetermined limits on the amount and volume of transactions and type of transactions.

36. Bank are permitted to cease the CDD process if they have a reasonable belief that performing the CDD process will tip off the customer that it considers that the transaction may be related to money laundering or the financing of terrorism. In such circumstances the bank may undertake the transaction provided that it immediately submits a suspicious transaction report to the FIU."

Reliance on third parties

37. (a) Bank may rely on third party intermediaries to perform the customer due diligence requirements of the Law and this Directive if the conditions in Section 24 of the Law are met.

(b) Before entering into a relationship with a third party, bank should have regard to the money laundering and terrorist financing risk associated with the country in which the third party is based.

(c) if the third party is identified as high risk, the bank should review any customer relationships introduced by the third party and terminate the relationship with the third party intermediary.

38. For purposes of Article 37 of this Directive, third party includes a person other than the bank and financial institution who conducts customer due diligence for the bank and financial institution where the third party should be subject to customer due diligence and record-keeping requirements consistent with the Law and is regulated, supervised or monitored by a supervisory authority. The third party may have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the bank or financial institution.

Shell banks and cross border correspondent banking relationships

39. Bank shall not enter into or continue a correspondent or business relationship with a shell bank in a foreign country that allows its accounts to be used by a shell bank.

40. Before entering into a cross-border correspondent banking relationship or other similar relationships, in addition to performing normal customer due diligence measures, bank shall:

(a) Gather sufficient information about the respondent bank and understand the nature of the respondent's business as required by section 26(a) of the Law.

(b) Evaluate the anti-money laundering and combating the financing of terrorism controls measures implemented by the respondent bank.

(c) *Based on publicly available information*, evaluate the reputation of the respondent institution and the quality of supervision to which it is subject, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.

(d) Obtain approval from senior management before establishing new correspondent relationships.

(e) Clearly understand and document the respective anti-money laundering and combating the financing of terrorism responsibilities of each bank.

(f) With respect to "payable-through accounts", be required to satisfy themselves that their respondents have performed CDD obligations on customers with direct access to the accounts and that respondents can provide relevant CDD information upon request.

New products and business practices

41. Bank shall identify, assess and, take appropriate measures to manage and mitigate the money laundering or terrorism financing risks that may arise in relation to:

(a) the development of new products and new business practices including new delivery mechanisms for products and services; and

(b) the use of new or developing technologies for both new and pre-existing products.

(c) The risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies.

Policies and Procedures on Wire or Electronic Transfers

42. Pursuant to Section 27(a) of the Law, bank that engage in cross border wire or electronic transfers shall include the following information on the wire or electronic transfers and ensure that the information remains with the wire or electronic transfers and related messages throughout the payment chain:

(a) Accurate originator and recipient information full name of the originator;

(b) The originator account number where such an account is used to process the transaction;

(c) The originator's address, or customer identification, or date and place of birth;

(d) The name of the recipient and the recipient account number where such an account is used to process the transaction.

43. If the bank is unable to comply with specifications prescribed in Article 42 of this Directive, it shall not execute the wire or electronic transfer.

44. Where several individual cross-border wire or electronic transfers from a single originator are bundled in a batch file for transmission to beneficiaries, banks need not apply requirements of Article 42 above in respect of originator information, provided that they include the originator's account number or unique transaction reference number which permits traceability of the transaction, and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

45. Domestic wire or electronic transfers, transactions should include the originator information required for cross border wire or electronic transfers, unless such information can be made available to the beneficiary institution and competent authorities through other

means, In such cases the ordering financial institutions need only include the originator's account number or where no account number exists, a unique transaction or reference number that allows the transaction to be traced back to the originator or the beneficiary.

46. Information on wire or electronic transfers shall be made available by the ordering bank within three business days of receiving the request either from the beneficiary bank or from the FIU.

47. For cross-border wire or electronic transfers, bank processing an intermediary element of the payment chain shall keep all wire or electronic transfer information including originator and beneficiary information.

48. Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire or electronic transfers from remaining with related domestic wire or electronic transfers information, the intermediary bank shall keep a record, for at least five years, of all the information received from the ordering bank or another intermediary bank.

49. Bank should have effective risk-based preventative procedures for determining:

(a) when to execute, reject, or suspend a wire or electronic transfers lacking required originator or required beneficiary information and consider reporting to the Financial Intelligence Unit;
(b) the appropriate follow-up action which may include restricting or terminating business relationships.

50. For wire or electronic transfers, a beneficiary bank shall verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with the record keeping requirements of the Law and this Directive.

51. In addition to the requirements of Article 49 of this Directive, in relation to wire or electronic transfers either ordering bank or beneficiary bank is required to report the following transactions to the FIU:

(a) A cross-border wire or electronic transfer in excess of USD 10,000 or the amount as required and determined by the Central Body from time to time;
(b) A domestic wire or electronic transfer in excess of 100 million kyats or the amount as required and determined by the Central Body from time to time;
(c) A transfer where the originator's information is incomplete or unavailable.

Suspicious Transaction Reporting Requirement

52. Where a bank has reasonable ground to believe that any transaction or attempted transaction is money or property obtained by illegal means or is related to money laundering or financing of terrorism, it must submit a report to the Financial Intelligence Unit on the form issued by the FIU in accordance with section 10(a) of the Law. The bank shall report as

soon as possible but no longer than three working days within 24 hours if it is situated in an urban centre or within 3 days if it is situated in a remote district.

Reporting of Threshold Transactions

53. Bank should submit a report to the Financial Intelligence Unit, on the form issued by the FIU in accordance with section 10(a) of the Law of transactions that exceed threshold amount defined by the Central Board in line with sections 32 and 34 of the Law. The bank shall report within 24 hours if it is situated in an urban centre or within 3 days if it is situated in a remote district.

Tipping-off Offences and Protection of Bank who report

54. Pursuant to section 33 and 66 of the Law, bank, their directors and employees and other responsible persons are prohibited from disclosing to a customer or any other person the fact that a report under Section 32 of the Law or any information has been reported to the Financial Intelligence Unit. This shall not preclude disclosures or communications between and among directors and employees of the bank, in addition to legal counsel.

55. Pursuant to section 59 of the Law, no criminal, civil, disciplinary or administrative proceedings for breach of banking or professional secrecy or contract shall lie against bank or their respective directors, principals, officers, partners, professionals or employees who in good faith submit reports or provide information in accordance with the provisions of the Law or this Directive.

Compliance, Audit, Screening and Training Staff

56. The compliance officer, appointed under Section 28(b) of the Law, should have appropriate experience and qualifications in the field of AML/CFT and have the authority to act independently and to report to senior management.

57. Bank shall supply the CBM and Financial Intelligence Unit with details of the compliance officer, including name, details on qualifications, address, contact number and email address. Bank should promptly inform the CBM and Financial Intelligence Unit of any change in the compliance officer.

58. The board of directors or such other management body of the bank shall periodically review the compliance officer's adherence to the requirements of the Law and this Directive.

59. The compliance officer shall submit regular reports including the following facts to the board of directors or management body:

(a) all suspicious transactions detected, and implications for the bank,

(b) measures taken by compliance staff to strengthen the bank's AML/CFT policies, procedures, systems and controls, results of any independent audit of AML/CFT systems,

(c) results of any onsite inspections conducted by the CBM or Financial Intelligence Unit,

(d) statement on remedial actions required to be implemented by the bank .

60. Bank must maintain an adequately resourced and independent audit function to ensure that the compliance officer and staff are performing their duties in accordance with its AML/CFT internal policies, procedures, systems and controls.

61. Bank must establish screening procedures to ensure appropriate standards when hiring employees and such procedures shall be approved by the Board of Directors or such other management body of the bank. Employee screening procedures must ensure that:

(a) employees have the high level of competence necessary for performing their duties;
(b) employees have appropriate ability and integrity to conduct the business activities of the bank;
(c) potential conflicts of interests are taken into account, including the financial background of the employee;
(d) fit and proper and code of conduct requirements are defined;
(e) persons charged or convicted of offences involving fraud, dishonesty or other similar offences are not employed by the bank.

Record keeping requirements

62. Pursuant to the requirements of section 23 of the Law, bank shall maintain records of the following information:

(a) Copies of all records obtained through the customer due diligence process including documents evidencing the identities of customers and beneficial owners, account files and business correspondence, for at least five years after the business relationship has ended or a transaction with a customer who does not have an established business relationship with the bank has been carried out;
(b) All records of transactions, both domestic and international, attempted or executed for at least five years following the attempt or execution of the transaction. Such records must be sufficiently detailed to permit the reconstruction of each individual transaction; and
(c) Copies of reports sent and related documents for at least five years after the date the report was made to the Financial Intelligence Unit.

Penalty and Actions

63. Any bank breaching the requirements of this Directive is liable to the penalties and sanctions as provided for in section 37 of the Law and Chapter XI of the Law.

General

64. This Directive replaces the Directive No.(21/2015) issued on October 2, 2015 by the CBM:

xxxxxxxxxx

For Governor

Soe Thein, Deputy Governor

Circulation;

State-owned Banks

Private Banks

Foreign Bank Branches

Schedule
Customer Identification Documents on CDD

Customer Identification Requirements for Customers

Bank shall obtain the following documents from the customers depending on the type of customer.

(A) Natural persons

1. Full name, including any aliases
2. National Registration Card/Citizen Scrutiny Card/Passport
3. Permanent and mailing address
4. Date of birth
5. Nationality
6. Occupation
7. Phone number (if any).
8. Photo
9. Name and account numbers of two introducers (existing account holders)

In the case of joint accounts, a bank shall obtain the above information on all parties to the account.

(B) Legal persons and Legal Arrangements including partnerships, limited liability partnerships and Trusts

1. Name of company
2. Address of head office.
3. Full address (including phone, fax)
4. Certificate of Incorporation, Memorandum of Association, Article of Association
5. Partnership Agreement
6. Trust deed
7. Name and address of Board of directors (phone number, if available)
8. Identification documents of Directors/Shareholders/Partners.
9. Identification documents of Settlors, Trustees, Protectors and beneficiaries with respect to trusts.
10. Board resolution authorizing opening and operation of the account
11. Authorization by Board of directors to Chief Executive Officer or other officers for conducting financial transactions.
12. Identification documents to identify the person authorized to represent the company/business in its dealings with the bank.

Bank shall verify the authenticity of the information provided by the company/business with the Directorate of Investment and Company Administration.

For foreign incorporated or foreign registered business entities, comparable documents should be obtained. Bank shall make all efforts to verify the documents supplied including requiring that they be certified by the Office of Foreign Affairs and endorsed by the Embassy of Myanmar.

(C) Non-Government Organization (NGO)

1. Name of Non-Government Organization.
2. Head Office Address.
3. Certification of registration.

4. Constitution of the NGO.
5. Name and address of Executive committee.
6. Telephone No.
7. Name and address of senior management
8. Registered address, if different to the principal place of business.
9. Executive committee's decision regarding opening of account.
10. Identification documents of directors/senior officers of the NGO.
11. Authorization for the operation of accounts financial transactions.
12. Identification documents to identify the person authorized to represent the NGO in its dealings with the bank.