



NCC Bank

नेपाल क्रेडिट एण्ड कमर्स बैंक लि.
Nepal Credit & Commerce Bank Ltd.

Administration Circular No: 57/2016

Date of Issue: December 16, 2016
(Poush 1, 2073)

Subject: Customer Due Diligence Procedure
(CDD Procedure) 2016

To: All the Staff Members of Nepal Credit
& Commerce Bank Ltd.

This is to inform all the staff members of NCC Bank that the Management Committee (Board) Meeting No. 587 held on November 28, 2016 (Marga 13, 2073) has approved the "Customer Due Diligence Procedure (CDD Procedure) 2016".

The Customer Due Diligence Procedure (CDD Procedure) 2016 has been attached herewith for your necessary record, information and implementation.

Ramesh Raj Aryal
Chief Executive Officer



NCC Bank

नेपाल क्रेडिट एण्ड कमर्स बैंक लि.
Nepal Credit & Commerce Bank Ltd.

Customer Due Diligence Procedure (CDD Procedure) 2016

*(Approved by the Management Committee Meeting No.587)
(Meeting held on November 28, 2016)*

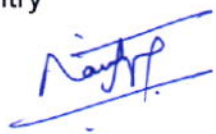
November 2016

1. Short Title

The Procedure will be cited as "Customer Due Diligence Procedure of Nepal Credit and Commerce Bank", (CDD Procedure).

2. Definitions

- 1) "Beneficial Owner" refers to the natural person(s) who ultimately owns or controls the Bank customer, in case the customer is legal person or arrangement, and/or the person on whose behalf a transaction is being conducted;
- 2) "Correspondent Banking" is the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank);
- 3) "Cross-Border transfer" means any wire transfer where the originator and beneficiary persons are located in different jurisdictions at the time of initiating the transfer. This term also refers to any chain of wire transfers that has at least one cross-border element;
- 4) "Domestic Transfer" means any wire transfer where the originator and beneficiary persons are located in the same jurisdiction at the time of initiating the transfer. This term, therefore, refers to any chain of wire transfers that takes place entirely within the borders of a single jurisdiction, even though the system used to effect the wire transfer may be located in another;
- 5) "High Risk categories" means customers, businesses or transactions that need to be subjected to more regular reviews, particularly against the Know-Your Customer information held by the Bank and the activity in the account. Such categories shall include, but not be limited to:
 - (a) Complex, unusual or large transactions,
 - (b) Relationships or transactions with countries known to have material deficiencies in anti money laundering and terrorist financing strategies,
 - (c) Politically Exposed Persons,
 - (d) Non-Resident Customers such as those staying in the country for less than one year or those in short visit or travel,
 - (e) "Legal Person" refers to a body corporate, foundation, partnership, non profit organization or association, or any similar body that can establish customer relationship with the bank or other financial institution, or otherwise own property;
 - f) "Money Laundering" shall have the meaning described as in Money (Asset) Laundering Act of the Country



- g) "Originator" is bank account holder, or where there is no account, the person that places an order with the bank or other financial institution to perform the wire transfer;
- h) "Payable-Through Accounts" refers to correspondent accounts that are used directly by third parties to transact business on their own behalf;
- i) "Person" means any natural or juridical person;
- j) "Politically Exposed Persons" shall have the meaning described as in Money (Asset) Laundering Act of the country
- k) "Shell Bank / Shell Company" means a bank/company that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision.
- l) "Senior Management" means a team of executives at the highest level who have the day-to-day responsibilities of managing the Bank;
- m) "Terrorist Financing" shall have the meaning described as in Money (Asset) Laundering Act of the country;
- n) "Wire Transfer" refers to any transaction carried out on behalf of an originator person through a bank or other financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another bank or financial institution. The originator and the beneficiary may be the same person.

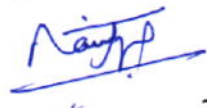
3. Customer Acceptance Policy, Procedure, and Compliance Arrangement

The Bank shall establish and maintain internal procedures, policies and controls to prevent money laundering and terrorist financing, and communicate these to their employees; at a minimum these procedures, policies and controls shall cover:

- a) explicit criteria for identification and acceptance of customers,
- b) appropriate risk management systems to determine whether a potential customer, an existing customer or beneficial owner is a Politically Exposed Person or high risk categories of customers,
- c) record retention techniques, methods and period ;
- d) unusual and suspicious transactions detection, techniques, methods and the reporting obligation;
- e) measures to be taken to prevent the misuse of technological developments in money laundering or terrorist financing schemes; and
- f) specific risks associated with non-face to face business relationships or transactions.

The Bank shall develop appropriate compliance management arrangements which at a minimum include:

- ii. designation of a compliance officer at the management level; and



- iii. ensure application of all laws related to anti-money laundering and combating terrorist financing; these directives; and internal policies, procedures and controls when establishing customer relationships and conducting ongoing due diligence.

4. Customer Identification and Due Diligence

- 1) The Bank may not keep anonymous accounts or accounts in fictitious names;
- 2) The Bank shall not enter into, or continue, correspondent banking relationships with shell banks/corporation.
- 3) The Bank shall undertake customer due diligence measures when:
 - i. establishing business relations with a customer;
 - ii. carrying out occasional cash transaction with a customer, which at a minimum exceeds certain sum fixed time to time;
 - iii. there is a suspicion of money laundering or terrorist financing, regardless of any exemptions or thresholds that are referred to under these directives; and
 - iv. they have doubts about the veracity or adequacy of previously obtained customer identification data.

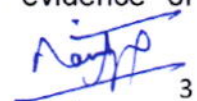
The Bank shall identify the customer, whether regular or occasional, natural or legal person or legal arrangement, and verify that customer's identity using as much as possible reliable, independent source documents, data or information.

5) Identification requirements for natural persons shall include, at a minimum:

- a) Given or legal name and all other names used;
- b) Permanent address;
- c) Telephone number, fax number and e-mail address, if available;
- d) Date and place of birth, if possible;
- e) Nationality;
- f) Occupation, public position held and/or name of employer;
- g) Type of account; and
- h) Signed statement certifying accuracy of the information provided.

6) For customers that are legal persons or legal arrangements, the Bank shall:

- a) take reasonable measures to understand the ownership and control structure of the customer and determine who the natural persons that ultimately own or control the legal person or arrangement are; this shall include those natural persons who exercise ultimate effective control over the legal person or arrangement;
- b) verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person;
- c) verify the legal status of the legal person or legal arrangement at a minimum by obtaining proof of incorporation or similar evidence of


3

establishment or existence and information concerning the legal person's or legal arrangement's :

- i. name,
- ii. legal form,
- iii. some form of official identification number such as tax identification number (if available),
- iv. address which includes the head office is located and if available, house number, mailing address, telephone number and fax number,
- v. names of directors, if applicable, and the chief executive officer,
- vi. provisions regulating the power to bind the legal person or arrangement;
- vii. the resolution of the board of directors any other authorized body or person to open an account; and
- viii. identification of those who have authority to operate the accounts.

- 7) In carrying out transactions with any person, the bank shall identify the ultimate beneficial owner and take reasonable measures to verify the identity of the beneficial owner using relevant information or data obtained from a reliable source such that the bank is satisfied that it knows who the beneficial owner is; particularly, for all customers, the bank shall determine whether the customer is acting on behalf of another person, and shall then take reasonable steps to obtain sufficient identification data to verify the identity of that other person.
- 8) Establishment of the bank's new business relationship with a politically exposed person shall be approved by a senior management member of the bank.
- 9) Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a politically exposed person, continuation of business relationship with such person shall be approved by a Branch Manager of the bank.
- 10) The Bank shall take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as politically exposed persons.
- 11) The Bank shall obtain information on the purpose and intended nature of the business relationship.
- 12) The Bank shall perform due diligence on high risk categories of customers, business relationships or transactions.

Risk Profile (High Risk Customers/ Low Risk Customers)

The Bank is required to conduct Customers Due Diligence if the customers falls within the definition of High Risk Customers, which are defined as under;

- a) Non-resident customers;



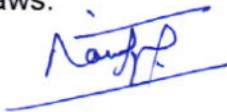
- b) Non-legal persons or arrangements including non-governmental organizations (NGOs) / Not for profit organizations (NPOs) and Trusts/charitable trust;
- c) Customer with links to offshore tax havens;
- d) High net worth customers with no clearly identifiable source of income;
- e) Customers dealing in high-value items;
- f) Politically Exposed Persons (PEPs). Those individuals who are or who have been entrusted with prominent public functions in a country or territory, for example heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned entities, important political party officials but not middle ranking or more junior individuals in these categories;
- g) Customers from or in countries where CDD/ KYC and anti-money laundering Regulations are lax and are not sufficiently applying Financial Action Task Force (FATF) recommendations: and
- h) Customers who have been refused by another financial institution (based on reasonable information).

For Low Risk Customers, NCC BANK may apply simplified or reduced CDD/ KYC measures.

A client may be considered under Low Risk category, if the identity of the customer(s) and the beneficial owner of a customer are publicly known or where adequate checks and controls exist.

Following cases may be considered as Low Risk Customers for application of simplified or reduced CDD/ KYC;

- a) Financial institutions provided they are subject to requirements to combat money laundering and terrorist financing and are supervised for compliance with those requirements; and
 - b) Public listed companies that are subject to regulatory disclosure requirements, Government administrations/entities.
 - c) Personal Account where the average balance in the account is below Rs. 1 million.
 - d) Person whose income source is apparent, e.g. salaried person
- 13) The Bank shall give special attention to business relationships and transactions with persons, including legal persons and other financial institutions, from or in countries which do not or insufficiently apply antimoney laundering and combating terrorist financing laws.



Enhanced Due Diligence Process for High Risk Clients (EDD)

Customer Enhanced Due Diligence is performed in situations when a new client is deemed to pose a higher money laundering risk.

Factors/Variables that Merit High Risk Status

There are various AML factors that can cause a client to be classified as high risk. A customer may pose a higher AML risk because of any of the following:

1. Customer's name is identified on a restricted persons list (i.e., OFAC's SDN List)
2. Customer originates from a high risk country
3. Customer does business in a high risk or sanctioned country
4. Customer does business in a high risk industry
5. Complex business and ownership structure
6. Suspicious behavior or activities
7. Transactions to/from higher-risk countries.
8. Other factor which deemed necessary for Enhance Due diligence

In addition, the Bank can perform the below additional reviews:

Additional name screening/negative news search

Approving EDD for High Risk Clients

After performing enhanced due diligence, the Bank has at least two options:

1. End the relationship and do not open the account
2. Accept the high risk relationship but implement a detailed monitoring plan and risk mitigation activities that can mitigate the Bank's risk exposure.

14. Account Monitoring

- 1) The Bank shall conduct Ongoing Due Diligence measure on existing customers and business relationships, including scrutiny of transactions undertaken throughout the course of that relationship, to ensure that:
 - a) the transactions being conducted are consistent with the bank's knowledge of the customers, their business and risk profile, and where necessary, the source of funds; and
 - b) documents, data or information collected under the due diligence process is kept up-to-date and relevant by undertaking reviews of

 6

existing records, particularly for higher risk categories of customers or business relationships.

- 2) Where the Bank is in a business relationship with a politically exposed person, they shall conduct enhanced ongoing monitoring.
- 3) The Bank shall pay special attention to all complex, unusually large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose such as significant transactions relative to a relationship, transactions that exceed certain limits, very high account turnover inconsistent with the size of the balance, or transactions which fall out of the regular pattern of the account's activity.
- 4) The Bank shall examine as far as possible the background and purpose of transactions.

15. Cross Border Correspondent Banking

- 1) With respect to cross-border correspondent banking and other similar relationships, Bank, in addition to performing normal customer due diligence measures, shall:
 - a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;
 - b) Assess the respondent institution's anti-money laundering and combating terrorist financing controls, and ascertain that they are adequate and effective;
 - c) Obtain approval from a senior management member of the bank before establishing new correspondent relationships; and
 - d) Document the respective anti-money laundering and combating terrorist financing responsibilities of each institution;
- 2) Where a correspondent relationship involves the maintenance of "payable through accounts", Bank shall be satisfied that:
 - a) their respondent financial institution has performed all the normal customer due diligence obligations set out in these directives on those of its customers that have direct access to the accounts of the correspondent financial institution; and
 - b) the respondent financial institution is able to provide relevant customer identification data upon request to the correspondent bank.
- 3) Where a correspondent bank fails to comply with national anti-money laundering and combating terrorist financing laws, Bank shall not open an account, commence business relations or perform transaction or shall\


7

terminate the business relationship with such correspondent financial institutions, and shall consider making a suspicious transaction report in relation to correspondent financial institutions.

- 4) The Bank shall satisfy themselves that respondent financial institutions in foreign countries do not allow business relationship with shell banks.

16. Wire Transfers

- 1) For all wire transfers, of amount fixed time to time or more, ordering banks shall be required to obtain and maintain the originator's:
 - a) Full name,
 - b) Account number or a unique reference number, if no account number exists,
 - c) Complete address, and
 - d) Date and place of birth (if possible).
- 2) For cross-border wire transfers of amount fixed time to time or more or for, the ordering financial institution or bank shall be required to include full originator information in the message or payment form accompanying the wire transfer.
- 3) Where several individual cross-border wire transfers of amount fixed time to time or more from a single originator are bundled in a batch file for transmission to beneficiaries in the country, the ordering foreign financial institution only needs to include the originator's account number or unique identifier on each individual cross-border wire transfer, provided that the batch file (in which the individual transfers are batched) contains full originator information that is fully traceable.
- 4) The Bank shall adopt effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information.

18. Exemptions

- 1) Identification of a customer does not need to be verified where the customer is itself a regulated bank or other financial institution that is subject to anti-money laundering and combating terrorist financing laws and regulations;
- 2) Credit and debit card transactions are exempted from standard customer due diligence, provided that they are not used as a payment tools to effect a money transfer.

19. Record Keeping

- 1) The Bank shall maintain all necessary records on transactions, both domestic and international, as stipulated in AML/KYC Policy of the Bank
- 2) Transaction records to be maintained by the Bank shall be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.



- 3) The Bank shall ensure that all customer and transaction records and information are available on a timely basis.

20. Reporting

The Bank shall report to Financial Intelligence Unit.

- 1) When it suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity;
- 2) Where there are reasonable grounds to suspect that funds are linked or related to, or to be used for terrorism, terrorist acts or by terrorist organizations or those who finance terrorism;
- 3) all cash deposits or withdrawals exceeding Rs. 1 million or transaction done on the same day, total of which exceed Rs. 1 million irrespective of branches the transaction conducted; and
- 4) all suspicious transactions, including attempted transactions regardless of the amount of the transaction.

21. Training programs

- 1) The Bank shall establish ongoing employee training programs which at a minimum incorporate:
 - a) Responsibilities under the Bank's arrangements for money laundering and terrorist financing prevention;
 - b) policies, procedures controls and practices for obtaining identification evidence; applying "know your customer" standard; account monitoring; enhanced due diligence; record keeping; and reporting knowledge or suspicion of money laundering and terrorist financing;
 - c) audit function to ensure the Bank's compliance with anti-money laundering and combating terrorist financing laws, directives, and internal policies and procedures;
 - d) Domestic laws and the Bank standards related to money laundering and terrorist financing;
 - e) Relevant typologies of money laundering and terrorist financing; and
 - f) Potential risks, including reputational, operational, legal and concentration risks of becoming involved in laundering the proceeds of crime or terrorist financing.
- 22) The Bank shall keep a record of training provided to the staff of the Bank.

