Da Afghanistan Bank

AML/CFT Responsibilities and Preventative Measures Regulation

Financial Supervision Department

2016

Table of Contents:

CHAPTER ONE

General Provisions

Basis

Article 1:

This Regulation is issued by the Da Afghanistan Bank pursuant to Article 69 of the Anti-Money Laundering and Proceeds of Crime Law.

Purpose

Article 2:

Da Afghanistan Bank requires all financial institutions as set out in Annex I to develop effective frameworks, preventive measures, systems, controls, and practices to manage their potential money laundering/terrorist financing (ML/TF) risks. It is important that financial institutions licensed to operate in Afghanistan have adequate controls and procedures in place so that they know the customers with whom they are establishing business relationships and dealings. Adequate due diligence on new and existing customers is a key part of these controls. Without adequate due diligence measures, financial institutions could be exposed to reputational, operational and legal risks, which can result in significant financial cost.

Goals and Objectives

Article 3:

(1) This regulation aims at protecting financial institutions from being abused by criminals and terrorists, thereby protecting their reputations and minimizing operational risk. Financial institutions are expected to perform their duties in the fight against money laundering and terrorist financing, particularly in the provisions of information that may lead to investigations and prosecutions of money launderers and terrorist financer. In that way, the integrity and solvency of the financial system is fostered, contributing to the financial security of the country.

(2) The objectives of this regulation:

1. Financial institutions will be required to have policies on customer acceptance that clearly identify when customers are to be rejected.
2. Financial institutions will be required to identify their customers properly.
3. Financial institutions will be required to submit reports to the FINTRACA on large cash transactions and suspicious transactions.
4. Financial institutions will be required to retain records of transactions.
5. Financial institutions will be required to have staffs that have been trained sufficiently to carry out their duties under this regulation.

(3) Adherence by financial institutions to the standards set by this regulation will be monitored by DAB through on-site examinations and off-site analysis of data.

Definitions

Article 4:

(1) Subject to paragraph (2) of this article, words and terms in this Regulation shall have the same meaning as the Anti Money Laundering and Proceeds of Crime law (AML&PC law).

Unless the subject or context otherwise requires, in this Regulation:

(2) "Senior management" comprise persons employed by a financial institution who exercise senior management responsibilities. Senior management responsibilities mean having primary responsibility for one or more of the following:

- High level decision making;

- Implementing strategies and policies approved by the Board;

- Developing processes that identify, manage and monitor risks incurred by the institution; and

- Monitoring the appropriateness, adequacy and effectiveness of the risk management system.

(3) "CDD" means Customer Due Diligence as defined in this Regulation.

(4) "Person" includes natural and legal persons.

(5) "FINTRACA" means Financial Transactions and Reports Analysis Center of Afghanistan established pursuant to Article 25 of the Anti-Money Laundering and Proceeds of Crime Law.

(6) "Threshold Reporting (Large Cash Transaction Report)" means report of the particulars of transactions (deposits, withdrawals or transfers) in excess of an amount specified in this regulation or any other applicable regulation.

(7) "Money Laundering" means as sub-paragraph 11, paragraph 1 of article 3 of Anti Money Laundering and Proceeds of Crime law.

(8) "Terrorist Financing" the offense as defined in Article 4 of Combating Financing of Terrorism Law.

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

(10) "Occasional Transaction" means any transaction that is initiated by a customer who is not a regular customer of the financial institution. In the case of depository institutions, all transactions initiated by customers who do not have a deposit account are to be considered occasional transaction.

(11) The terms "Trust" and Trustee" should be understood as described in and consistent with Article 2 of the Hague Convention on the law 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 non-professional (e.g. a person acting without reward on behalf of family).

(12) "Beneficiary" for purposes of a trust means, 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. All trusts (other than charitable or statutory permitted non-charitable trusts) are required to have ascertainable beneficiaries.

(13) "Ordering bank" means the financial institution which initiates the wire transfer and transfers of funds upon receiving the request for a wire transfer on behalf of the originator.

(14) "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 transfer.

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

(16) "Law" means AML & PC law.

CHAPTER TWO

Policies, Procedures Risk Assessments and Identification

Policies and procedures

Article 5:

(1) Financial Institutions should have internal polices, procedures, systems, controls and customer acceptance policy that clearly indicates situations when a customer will be rejected, and must be able to demonstrate to the satisfaction of Da Afghanistan Bank examiners that the policy has been implemented.

(2) The internal policies, procedures, systems, and controls to combat money laundering and terrorism financing developed by financial institutions should address the following requirements:

1. Risk evaluation of the customer, products, services, geographic locations, and delivery channels as well as transactions.

2. Identification and verification of the customer and beneficial owner, including walk-in/occasional customers, and politically exposed person(s).
3. Application of customer due diligence measures

4. Maintaining records and information obtained in the CDD process and information of transactions.
5. Monitoring of transactions, including monitoring to identify unusual or suspicious transactions.
6. Reporting to FINTRACA of threshold transactions.
7. Reporting to FINTRACAof suspicious transactions.
8. Ensuring that internal policies, procedures, systems and controls are subject to independent testing and review.
9. The appointment of a compliance officer at senior management level to ensure compliance with the provisions of the Anti-Money Laundering and Proceeds of Crime Law and this Regulation.
10. Ensuring high standards as set out in fit and proper requirements while recruiting employees. This should include separate fit and proper requirements for employees in management positions or in positions perceived to have greater exposure to money laundering or terrorist financing.
11. Establishing training programs and providing on-going trainings to all new and existing employees, directors, board members, executive or supervisory management.
12. Other arrangements as prescribed by DAB or FINTRACA.

(3) The internal policies, procedures, systems and controls should be consistent with the financial institution's size, nature ,risks, and complexity of operations and should be adopted by the bank's or financial institution's board of directors and be applicable to all domestic and foreign branches and majority-owned subsidiaries of the financial institution.

(4) Financial institutions must designate one individual as an "AML Officer" having primary responsibility for development and implementation of the anti money laundering measures contained in this regulation. a different individual must be designated as having responsibility for auditing the implementation by the AML officer of the policies and procedures developed. In particular, the system of internal controls must ensure that the necessary reports are filed with the FINTRACA. This audit function should report directly to the Board of Supervisors and its reports should include examples, if any, of the AML officer's failure to implement these measures.

Conducting risk assessments

Article 6:

(1) Financial institutions shall assess and understand their money laundering and terrorism financing risks, including of new products or technologies. The risk assessment and any underlying analysis and information shall be documented in writing, be kept up-to-date and readily available for Da Afghanistan Bank to review at their request.

(2) Financial institutions should have in place processes to identify, assess, monitor, manage and mitigate money laundering and terrorism financing risks.

(3) Financial institutions shall document the risk assessments in order to be able to demonstrate their basis, keep these assessments up to date, and make the documents of the processes and the risk assessment documentations available to Da Afghanistan Bank upon request.

(4) Financial institutions shall consider the following factors, among others in accordance with the pertinent information, when preparing their risk assessments. :

1. Customers (i.e. nature of their business, occupation, or anticipated transaction activity, among others);

2. Origin and source of the customer's funds;

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

4. Geographic location (i.e. countries or domestic geographic areas in which customers operate or the place of origination or destination of transactions); and

5. Delivery channels (i.e. the risks that arise from the channels used to deliver products and services).

6. The purpose of an account or relationship:
Risks associated with transactions, including the size of deposits or transactions undertaken by a customer; the frequency of transactions or duration of the relationship; whether the transactions is outside the scope of normal transactions conducted by the customer or whether the transaction originated or is destine for a high risk jurisdiction

(5) Possible factors of high risk situations where financial institutions should apply enhanced CDD measures are set out in Annex III.

(6) Possible factors of lower risks where financial institutions may apply simplified due diligence include but are not limited to those situations set out in Annex III:

(7) In designing and implementing customer identification programmes, financial institutions should take into consideration the risks set out above. Financial institutions, on the basis of the evaluation pursuant to this Chapter shall adopt the following measures to manage the risk:

1. To obtain additional information on the customer, beneficial owner, beneficiary and transaction.
2. To establish a risk profile on customers and transactions. The customer profile should be based upon sufficient knowledge of the customer (and beneficial owner(s) as applicable), including the customer's anticipated business with the bank or financial institution, and where necessary the source of funds and source of wealth of the customer.
3. To apply enhanced customer due diligence to high-risk customers.

4. To update more regularly the information on all customers.
5. To adopt other measures as may be prescribed by Da Afghanistan Bank or the FINTRACA.

Customer Identification Requirements

Article 7:

(1) Financial institutions shall not maintain or open an anonymous account or an account in fictitious names.

(2) Financial institutions must set up a registration system for the identification of their clients and establish the identity of clients when performing any transaction for them.

(3) Financial institutions must ensure that they know the true identity of their customers, including beneficial owners. Customer due diligence should be carried out in the following cases:

1. Before establishing a business relationship with a customer or opening an account except for the situations provided in Article (11) of this regulation.

2. Before a non-bank financial institution carrying out a transaction for an occasional or walk-in customer (a customer who is not in an established business relationship with the financial institution), when the transaction involves an amount equal to or above 50000 AFS or its equivalent in other currencies, whether conducted as a single transaction or several transactions that appear to be linked;

3. Banks must not carry out occasional transactions in excess of AFS 500,000 on behalf of customers who refuse to identify themselves at all or refuse to disclose and document the source of their funds.

4. Before carrying out domestic or international wire transfers as provided in Article (17) of this regulation;

5. Whenever doubts exist about the veracity or adequacy of previously obtained customer identification data; and
6. Whenever there is a suspicion of money laundering or terrorist financing.

(4) Financial institutions shall carry out the following customer due diligence measures:

1. Identify and verify the identity of the customer and beneficial owner using reliable, independent source documents, data or information.

2. Verify that any person acting on behalf of the customer is authorized to do so and identify and verify the identity of that person.

3. Understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.

4. To the extent possible, obtain the customers' tax identification number (TIN) and tax statements and in addition, in the case of legal persons, audited financial statements and details as shall be specified by Da Afghanistan Bank or the regulatory agency.

5. Monitor the business relationship on an ongoing basis and examine any transactions carried out to ensure they are consistent with their knowledge of the customer, commercial activities and risk profile, and where required, the source of funds.

6. For legal persons, understanding and documenting the ownership and control structure of the customer.

(5) For customers who are natural persons, financial institutions must verify the identity required using reliable, independent source documents, data, or information as outlined in Annex II of this Regulation.

(6) For customers who are legal persons or legal arrangements, financial institutions must identify the customer and its beneficial owners, including by understanding the nature of its business, and its ownership and control structure. Financial institutions should obtain and verify the information required using reliable, independent source documents, data, or information as outlined in Annex II of this regulation. Where relevant, customer identification requirements for natural persons can be applied to identifying customers who are legal persons and arrangements. Procedures established in this Regulation relating to the identification and verification of natural persons who are individual customers are similarly applicable to beneficial owners of legal persons and arrangements.

(7) Financial institutions should verify whether any natural person is purporting to act on behalf of a customer who is legal persons or legal arrangements.

(8) For legal persons, the following information should be obtained at a minimum:

1. Name, legal form and proof of existence of the legal persons;

2. Location of the principal place of business of the legal person;

3. Resolution of the Board of Directors to open an account and identification of those individuals who have authority to operate the account and names of relevant persons holding senior management positions.

4. Mailing and registered address of legal person;

5. Nature and purpose of the business;

6. The identity of the beneficial owner;

(9) Legible file copies should be taken of the relevant identification and supporting documentation for all customers both natural and legal persons. The customer's signature or finger print should be obtained on each page of such copies.

(10) Da Afghanistan Bank may set out in guidelines additional identification and verification requirements for customers to be applied by financial institutions.

Identification and Verification of Beneficial Owner

Article 8:

(1) Financial institutions must take reasonable measures to determine if a customer is acting on his/her own or on behalf of one or more beneficia1 owners. If a financial institution determines that the customer is acting on behalf of one or more beneficial owners, financial institutions should take steps to verify the identity of the beneficial owner(s) by using relevant information or data obtained from a reliable source such that the financial institution is satisfied that it knows the identity of the beneficial owner(s). The information to be obtained on a beneficial owner should be consistent with the requirements outlined in Annex II of this Regulation.

(2) If a customer is a company listed on a stock exchange, a financial institution 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, financial institutions should only obtain customer identification documents on the company itself as outlined in Annex II of this Regulation.

(3) For customers that are other legal entities or legal arrangements, financial institutions should take adequate measures to understand the ownership and control structure of the customer, including the ultimate natural person who owns or controls it as described below:

1. With respect to such legal entities identification should be made of each natural person that:

   - Owns or controls directly or indirectly more than 10% of the legal entity;
   - Is responsible for the management of the legal entity; or
   - Exercises control of the legal person through other means.

2. With respect to legal arrangements, identification should be made of the settlor, trustee, protector, beneficiary or of persons in similar positions.

CHAPTER THREE
Politically Exposed Persons and risk Measure

Politically Exposed Persons
Article 9:

(1) Financial institutions shall establish appropriate risk management systems to determine whether a customer or beneficial owner is a politically exposed person (PEP) and if so, apply the following additional customer due diligence measures:

1. obtain approval from senior management before establishing or continuing a business relationship with such a person or beneficial owner;
2. take all reasonable measures to identify the source of wealth and funds of customers and beneficial owners identified as PEPs; and
3. apply enhanced ongoing monitoring to the business relationship.

(2) Procedures for determining whether a customer or beneficial owner is a PEP, should include:

1. seeking relevant information from the customer or beneficial owner;

2. accessing and reviewing available information from any reliable source about the customer or beneficial owner;

3. accessing and reviewing commercial electronic databases of PEPs, if available

4. Accessing and reviewing the FINTRACA's non-confidential information if available on PEPs which should not be the sole source of information.

Enhanced CDD ML/TF Risks Measures
Article 10:

(1) Financial institutions should examine, including by seeking additional information from the customer , the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Such information to be obtained can include information on the nature or reason for the transaction.

(2) Where the risks of money laundering or terrorism financing are higher, financial institutions should conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

(3) Enhanced CDD measures that should be applied for higher-risk business relationships include, but are not limited to the following:

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

2. Obtaining additional information on the intended nature of the business relationship.

3. Obtaining information on the source of funds or source of assets of the customer.

4. Obtaining information on the reasons for intended or performed transactions.

5. Obtaining the approval of senior management to commence or continue the business relationship.

6. 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.

7. Carrying out the first payment through an account in the customer's name with a bank subject to similar CDD measures.

(4) Enhanced CDD should be applied to higher risk customers at each stage of the CDD process and on an on-going basis.

(5) Enhanced CDD procedures for business relationships with natural persons not physically present for the purpose of identification should include:

1. certification of documents in line with relevant Laws and Regulations;

2. requisition of additional documents and development of independent verification measures and/or contact with the customer.

Simplified CDD ML and TF Risks
Article 11:

(1) Financial institutions may apply simplified customer due diligence procedures upon undertaking a documented risk assessment of the customer relationship.

(2) The general rule is that customers must be subject to the full range of customer due diligence measures as provided in this Regulation. In certain circumstances where the risk of money laundering or terrorist financing is lower, as determined by a risk assessment undertaken by the financial institution, where information on the identity of the customer and the beneficial owner of a customer is publicly available, or where adequate checks and controls exist elsewhere in national systems, simplified measures may be employed.

(3) Financial institutions shall not apply simplified CDD measures whenever there is a suspicion of money laundering or terrorism financing or when the customer has a business relationship with or in countries as mentioned in Annex III of this regulation.

(4) Where requested by DAB, financial institutions shall submit the underlying risk assessment and basis for the application of simplified customer due diligence and shall make the documents of the assessment processes and procedures related to risk assessment available to Da Afghanistan Bank.

1. The simplified CDD measures should be commensurate with the risk factors.

2. Where the risks have been identified as low, possible simplified CDD measures could include, but are not limited to the following:

   - Reducing the frequency of customer identification updates.

   - Reducing the degree of on-going monitoring and scrutinising transactions.

Delayed Customer Identification Verification

Article 12:

(1) Financial institutions may engage in the business relationship with the customer prior to the completion of the customer verification process outlined in article (6) of this Regulation provided all of the following circumstances are met:

   1. when the verification occurs as soon as reasonably practicable.

   2. when it is essential not to interrupt the normal conduct of business.

   3. when the ML and TF risks are effectively managed.

(2) Financial institutions shall adopt risk management procedures with respect to the conditions under which a customer may utilize the business relationship prior to verification;

(3) These procedures should include a set of measures to manage the ML and TF risks and such measures could include:

1. limitation of the number, types and or amount of transactions that can be performed;
2. the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

(4) Financial institutions 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.

Additional requirements for Customer Information

Article 13:

(1) Financial institutions must gather and maintain customer and beneficial owner(s) information throughout the course of the business relationship. Documents, data, or information collected under the CDD process should be kept up to date and relevant by undertaking reviews of existing records at appropriate times as determined by the financial institution, for example when:

1. A significant transaction is to take place;

2. There is a material change in the way the account is operated or transactions begin to deviate from the usual patterns;

3. Information held on the customer is insufficient to enable the financial institution to understand the nature of the business relationship or transactions being conducted.

(2) In addition to the requirements of Article 12 of the AML & PC Law, in the case of legal persons, financial institutions must ensure:

1. that business and company registration and licensing documents are current and remain valid throughout the duration of the relationship.

2. that they obtain updated financial statements from customers.

3. that taxation information (copy of tax returns and certification) is obtained and updated on an annual basis.

4. that all transactions conducted by customers are accompanied by supporting documentation, such as customs certifications confirming the value of the goods.

(3) Financial institutions should apply the CDD requirements of this regulation to existing customers on the basis of materiality and risk.

(4) The KYC/ account opening forms should be prepared by financial institution, and filled out by customer in any of national languages of Afghanistan unless the customer is a foreign citizen.

(5) Notwithstanding the provisions of other paragraphs of this Article, financial institutions should renew/ update the KYC forms of any customer at least on yearly basis.

CHAPTER FOUR

Ongoing Monitoring of Customer Transactions, Customer and correspondent banking relationship

Ongoing Monitoring of Customer Transactions
Article 14:

(1) Financial institutions should implement systems, for example automated systems, to monitor on an ongoing basis customer transactions and the relationship with the customer. Monitoring must include the scrutiny of customer transactions to ensure that they are being conducted in line with the financial institution's knowledge of the customer and the customer risk profile and, where necessary, the source of funds and wealth, and may include predetermined limits on the amount and volume of transactions and type of transactions.

(2) Financial institutions must monitor customers' account activity, on a regular, reasonable schedule, to be able to establish patterns, the deviation from which may indicate suspicious activity.

Termination of Customer Relationship
Article 15:

(1) If a financial institution is unable to comply with the CDD required for a customer, including, on the basis of materiality and risk, on existing customer relationships established prior to the enactment of this regulation, they should terminate the customer relationship and consider filing a report with the FINTRACA.

(2) Where a financial institution is unable to verify the identity of the customer and beneficial owner(s), it shall refrain from opening the account or commencing the business relationship or carrying out the transaction. In such cases, the financial institution shall consider filing a suspicious transaction report to the FINTRACA.

Reliance on third parties
Article 16:

(1) Financial institutions may rely on third party intermediaries to perform the CDD requirements of this regulation if the following conditions are met:

1. They are satisfied that the third party is regulated, supervised or monitored for and has measures in place for compliance with the customer due diligence and record keeping requirements;
2. They can immediately obtain all required customer due diligence information; and
3. They are satisfied that copies of identification data and other documents relating to customer due diligence measures will be made available from the third party upon request and without delay.

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

(3) The ultimate responsibility for customer identification and verification shall remain with the financial institution relying on the third party.

Shell banks and cross border correspondent banking relationships

Article 17:

(1) Financial institutions shall not enter into or continue a correspondent or business relationship with a shell bank and they must satisfy themselves that respondent financial institutions do not permit their accounts to be used by shell banks.

(2) Before entering into a cross-border correspondent banking relationship or other similar relationships, in addition to performing normal customer due diligence measures financial institutions shall:

1. Gather sufficient information about the respondent bank.

2. Understand the nature of the respondent's business.

3. 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.

4. Evaluate the anti-money laundering and combating the financing of terrorism controls implemented by the respondent bank.

5. Obtain approval from senior management before establishing new correspondent relationships.

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

(3) With respect to payable-through accounts, financial institutions should be required to satisfy themselves that the respondent bank:

1. has performed CDD obligations on its customers that have direct access to the accounts of the correspondent bank;

2. is able to provide relevant CDD information upon request to the correspondent bank.

(4) These requirements should also be applied to cross border correspondent banking and similar relationships established prior to the enactment of the Anti-Money Laundering and Proceeds of Crime Law and issuance of this Regulation.

CHAPTER FIVE

Policies and Procedures on Wire Transaction and Reporting Requirements

Policies and Procedures on Wire Transfers
Article 18:

(1) Financial institutions that engage in cross border wire transfers 50,000 AFS or equivalent in other currencies, shall include accurate originator and beneficiary information on wire transfers and related messages and ensure that the information remains with the wire transfer or related messaged throughout the payment chain. Information accompanying all wire transfers should always contain:

1. The full name of the originator;

2. The originator 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;

3. The originator's address, or customer identification, or date and place of birth;

4. The name and address of the beneficiary and the beneficiary account number or a unique identification number where such an account or number is used to process the transaction.

(2) Financial institutions shall obtain necessary supporting documents, in addition to information obtained under paragraph (1) above, in case of cross border wire transfers equal to or exceeding AFS 1,000,000 or its equivalent in other currencies.

(3) For cross border transfers bellow 50,000 AFS or its equivalent in other currencies, financial institutions should ensure that they are always accompanied by:

1. Name of originator and
2. Account number or unique transaction number.

(4) If the financial institution is unable to comply with these requirements, it shall not execute the wire transfer and consider submitting a suspicious transaction report to the FINTRACA.

(5) Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, financial institutions may not apply requirements of article 17 paragraph(1) of this regulation 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.

(6) For domestic wire transfers (including transactions using a credit or debit card as a payment system to affect a money transfer), the ordering institution must include either:

1. full originator information in the message or payment form accompanying the wire transfer; or
2. only the originator's account number, where no account number exists, a unique identifier, within the message or payment form.

(7) Information on wire transfers should be made available by the ordering bank within three business days of receiving the request either from the beneficiary financial institution or from the FINTRACA .

(8) Financial institutions should ensure that non-routine wire transfers are not batched where this would increase the risk of money laundering or terrorism financing.

(9) For cross-border wire transfers, financial institutions processing an intermediary element of the payment chain should keep all wire transfer information including originator and beneficiary information.

(10) Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with related domestic wire transfer information, the intermediary financial institution should keep a record, for at least five years, by the receiving intermediary financial institution of all the information received from the ordering financial institution or another intermediary financial institution.

(11) Financial institutions should have effective risk-based procedures for determining:

1. when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information and considering reporting to the FINTRACA;
2. the appropriate follow-up action which may include restricting or terminating business relationships.

(12) For wire transfers, a beneficiary financial institution should 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 this regulation.

(13) For the purposes of this Chapter,

1. "Beneficiary" means the natural or legal person who is identified by the originator as the receiver of the requested wire transfer and also refers to the term "recipient" as it appears in the AML & PC law article 3.3.2.

2. Beneficiary financial institution" means the financial institution which receives the wire transfer from the ordering bank directly or through an intermediary financial institution and makes the funds available to the beneficiary.

Suspicious Transaction Reporting Requirement

Article 19:

(1) Financial institutions must, as soon as possible but no later than 3 working days, after forming a suspicion that any transaction or attempted transaction, regardless of value, involves proceeds of crime or funds related or linked to or to be used for money laundering or terrorism financing, report to the FINTRACA.
(2) Financial institutions should report details of suspicious transactions to the FINTRACA in the prescribed form as set out in a guideline to be issued by FINTRACA.
(3) Suspicious transaction report should be submitted to FINTRACA in any of official languages of Afghanistan together with all necessary supporting documents including but not limited to: updated customer's KYC and account opening forms, updated account/s statement/s, identification documents (Tazkira or passport, Business license and etc) and other relevant documents support the reasons for forming suspicion about the customer.
(4) While forming suspicion about a customer, the financial institution should conduct preliminary analysis on its customers based on all information available to it including the records of its previous transactions, and other documents provided to it by customers since establishment of its business relationship with Financial Institution, and include the result of such analysis in its report to FINTRACA.
(5) If FINTRACA determines that the STR quality is not at a level satisfactory to work on it, or missing necessary supporting documents set out in paragraph 4 of this Article, FINTRACA may reject the receipt of the STR and notify the financial institution of reasons of such rejection, and the financial institution should rectify the deficiencies and inform the FINTRACA.

Threshold Reporting Requirements

Article 20:

(1) Banks shall report the particulars of transactions (deposits, withdrawals or transfers) in excess of AFS 1,000,000 or its equivalent to other currencies to the FINTRACA no earlier than the first business day of the month and no later than the fifth business day of a month following to the month during which the transaction occurred.

(2) Other financial institutions should report their LCTR according to the threshold and timeframe prescribed in their relevant Regulations or circulars issued by FinTRACA.

(3) Financial institutions should report details of transactions to the FINTRACA in the prescribed form as set out in a guideline to be issued by FINTRACA and may be updated from time to time.

(4) Financial institutions should include all details required by FINTRACA under paragraph 3 of this Article in a precise manner. In case of submitting deficient or carelessly filled out LCTR forms to FINTRACA, FINTRACA can apply the sanctions provided for in article 24 of AML&PC Law on the financial institution.

Tipping-off Offences

Article 21:

(1) Financial institutions, their directors and employees are prohibited from disclosing to a customer or any other person the fact that a report under Article (18) AML & PC law and Article (18) of this regulation or any information related to the FINTRACA or to any money laundering or terrorism financing investigation. This shall not preclude disclosures or communications between and among directors and employees of the bank or financial institution, in addition to lawyers, competent authorities, and the public prosecution.

(2) No criminal, civil, disciplinary or administrative proceedings for breach of banking or professional secrecy or contract shall lie against banks or financial institutions 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 this regulation and the AML & PC Law.

New products and business practices

Article 22:

(1) Before launching new products and business practices or using new technologies , financial institutions should identify, assess and, take appropriate measures to manage and mitigate the money laundering or terrorism financing risks that may arise in relation to:

1. the development of new products and new business practices including new delivery mechanisms for products and services; and
2. the use of new or developing technologies for both new and pre-existing products.

Internal Policies, Procedures, Systems and Controls

Article 23:

(1) The compliance officer and other compliance staff should have timely access to customer identification data and other CDD information, transaction records, and other relevant information. The compliance officer 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.

(2) The financial institution should supply Da Afghanistan Bank with details of the compliance officer, including name, details on qualifications, address, contact number, email address and get the approval of Da Afghanistan Bank for Chief Compliance Officer position. The bank or financial institution should promptly inform Da Afghanistan Bank of any change in the compliance officer.

(3) The board of directors of the financial institution shall periodically review the financial institution's compliance with the requirements of the Anti-Money Laundering and Proceeds of Crime Law and this Regulation. Such regular reports to the board of directors should include a statement on all suspicious transactions detected, implications and measures taken by compliance staff to strengthen the financial institution's AML/CFT policies, procedures, systems and controls. Reports on suspicious transactions should be general and not include any information on specific transactions or customers. The board should also be informed of the results of any onsite inspections conducted by Da Afghanistan Bank, including remedial actions required to be implemented by the financial institution.

(4) Financial institutions must maintain an adequately resourced and independent audit function to ensure that the compliance officer and staff of the financial institution are performing their duties in accordance with the bank's or financial institution's AML/CFT internal policies, procedures, systems and controls.

(5) Financial institutions' external auditors shall report on the adequacy of the bank's or financial institution's internal control systems and include an explicit opinion on the financial institution's adherence to all applicable local laws, ministerial decisions and Da Afghanistan Bank regulations and Instructions, as well as the financial institution's adherence to its own policies, procedures, systems and controls. This report shall be made available to the Da Afghanistan Bank on request.

(6) Financial institutions must establish screening procedures when hiring employees. Such screening procedures should include fit and proper requirements to be applied when hiring employees. More stringent fit and proper requirements are required for employees in management positions or in positions perceived to have greater exposure to money laundering or terrorist financing. Employee screening procedures and fit and proper requirements must ensure that:

1. employees have the high level of competence necessary for performing their duties as set out in their job descriptions;

2. employees have appropriate ability and integrity to conduct the business activities of the bank or financial institutions;

3. potential conflicts of interests are taken into account, including the financial background of the employee;

4. fit and proper and code of conduct requirements are defined;

5. Persons convicted of offences involving fraud, dishonesty, money laundering or other similar offences are not employed by the bank or financial institution, subject to laws of Afghanistan.

CHAPTER SIX

Record Keeping Requirements, Counter Measures, Penalty and Action

Record Keeping Requirements

Article 24:

Financial institutions shall maintain records of the following information:

1. Copies of all records obtained through the customer due diligence process under 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;

2. All records of transactions, both domestic and international, attempted or executed for at least five years
   - after the attempt or execution of the transaction;
   - after the business relationship has ended
   - after a transaction with a customer who does not have an established business relationship with the bank has been carried out; which is the longest.
3. Such records must be sufficiently detailed to permit the reconstruction of each individual transaction;

4. Copies of suspicious transactions reports sent and related documents for at least Ten years and for other reports and its related documents at least five years after the date the report was made to the FINTRACA;

5. The risk assessment and any underlying information for a period of five years from the date the assessment was carried out or updated.

Counter Measures on High Risk Countries

Article 25:

(1) Financial institutions shall implement measures imposed by Da Afghanistan Bank issued under Article 14 paragraph(4) of the AML & PC Law. The measures that Da Afghanistan Bank may impose include, but are not limited to the following:

1. applying specific elements of enhanced due diligence such as obtaining additional information on the customer, purpose of transactions, nature of the business relationship and the source of funds or wealth of the customer;

2. obtaining senior management approval to continue the relationship; and,

3. increased monitoring of transactions; and

4. Reviewing, amending or if necessary terminating correspondent banking relationships.

(2) Da Afghanistan Bank may take certain actions including, but not limited to the following:

1. Imposing additional reporting requirements on financial institutions;

2. Refusing the establishment of subsidiaries or branches or representative offices of financial institutions from the country identified under Article 14 paragraph(4) of the AML & PC Law;

3. Prohibiting Afghani financial institutions from establishing branches or representative offices in the country identified under Article 14 paragraph(4) of the AML & PC Law;

4. Requiring financial institutions to limit business relationships or financial transactions with the country identified under Article 14 paragraph(4) of the AML & PC Law or persons in that country;

5. Increasing supervisory examinations and/or external audit requirements for branches and subsidiaries of financial institutions from the country identified under Article 14paragraph(4) of the AML & PC Law operating in the Islamic Republic of Afghanistan; and

6. Requiring increased external audit requirements for Afghan's financial groups with respect to any of their branches and subsidiaries located in the country identified under Article 14paragraph(4) of the AML & PC Law.

(3) Financial institutions are required to report any transactions with countries identified under Article 14 paragraph (4) of the AML & PC Law to the FINTRACA.

Compliance with CFT Regulation

Article 26:

(1) Financial institutions are required to develop and implement procedures to ensure compliance with the requirements of the Counter Financing of Terrorism Law and CFT Regulations, Terrorist Asset Freezing Procedure including:
    1. Procedures to freeze without delay funds, property and assets held by the financial institution, including in safe custody, in response to directions received from competent authorities pursuant to the Counter Financing of Terrorism Law;
    2. Procedures to monitor attempted access by customers or other parties to the funds, property or assets;
    3. Procedures to allow access to the funds, property or assets held in response to directions from competent authorities;
    4. Procedures to unfreeze funds, property or assets in response to directions from competent authorities.

(2) Financial institutions are required to submit a report to FINTRACA in relation to any attempt to access the funds, property or assets which are subject to an order under the Counter Financing of Terrorism Law. Such reports should be submitted without delay.

Confidentiality

Article 27:

Financial institutions and their staff shall maintain confidentiality, and not disclose information concerning their anti-money laundering activities to their clients or to others, except to the FINTRACA. The exception is that they may disclose to other financial institutions or to their professional associations information about potential clients or transactions that they have refused. In particular, financial institutions must not disclose to clients that they have filed suspicious transactions reports about their activity. Financial institutions are advised to maintain signage in a prominent place or to hand out written notices to their customers that they are required to report all large cash transactions to the Financial Intelligence Unit. Staff may also orally advise each customer at the time the transaction is initiated.

Staff Training

Article 28:

Financial institutions are responsible for training their staff in the requirements of this regulation and continually updating the skills of their staff as requirements and situations change. This training should include real-world examples of transactions that constituted money laundering and terrorist financing, and an awareness of the role that staff play in the overall process of detecting and punishing money launderers and terrorist financers.

On-site Supervision
Article 29:

Examination personnel of the Financial Supervision Department of DAB will conduct reviews of financial institutions' compliance with these regulations as a part of their regularly-scheduled on site examinations. Findings by the examiners that the institution's policies are inadequate or poorly implemented will result in a low rating for the "M" component of the "CAMELS" rating system for a bank, and the possibility of enforcement action against all types of financial institutions.

Penalty and Actions
Article 30:

Any financial institution breaching this Regulation is liable to the sanctions as provided for in Article 24 and Article 51 of the AML & PC Law, and sanctions in the Banking Law and other relevant laws of Afghanistan.

In cases where a financial institution is found to have committed any of the following acts, the Financial Supervision Department and FINTRACA shall request it to correct the problem within a specified period of time, and issue enforcement actions that may include license revocation, fines, the requirement of an external audit, or the removal of administrators and the replacement with administrators acceptable to DAB. Violations leading to enforcement actions include, but are not limited to:

1. Failing to set up an internal control system for anti-money laundering activities
2. Failing to designate an AML officer.
3. Failing to identify customers properly.
4. Disclosing to customers or potential customers that reports are being filed about them to the FINTRACA.
5. Failing to maintain account information and transactions records on clients, and updating the information.
6. Failing to report large cash transactions or suspicious transactions to the FINTRACA, as required.

In addition, financial institutions that knowingly participate in money laundering or terrorist financing, and the administrators of these financial institutions, will be punished according to the provisions of Anti Money Laundering or Terrorist Financing Laws.

Cooperation with law enforcement
Article 31:

Financial Institutions shall cooperate and coordinate their anti-money laundering activities with FINTRACA and cooperate with the FINTRACA in any freezing or transferring the deposits of clients, according to the relevant provisions in law and regulation.

Responsibilities of foreign branches of financial institutions licensed in Afghanistan
Article 32:

The foreign branches of financial institutions licensed in Afghanistan shall abide by the provisions of laws governing anti-money laundering of the country or region where they are located, and provide cooperation and assistance to the anti-money laundering efforts of law enforcement officials of their host country, according to the laws of the host country.

Responsibilities of professional associations of financial institutions
Article 33:

The Afghanistan Banking Association (ABA), the Financial Companies Association of Afghanistan, the Union of MSPs and FXDs and other financial self-disciplinary organizations may draft working guidelines or codes of conduct for their members concerning anti money laundering activities, inline with this regulation. they may discipline or suspend the membership of financial institutions that do not comply with these guidelines. These organizations are also expected to encourage information-sharing among their members concerning the details of customers or individual transactions that have been refused.

Other
Article 34:

The Da Afghanistan Bank and FinTRACA may issue sector specific guidelines or circulars to financial institutions to provide further guidance on the implementation of the requirements of the Law and this Regulation.

Effective Date of Regulation
Article 35:

This regulation is effective immediately after adoption by supreme council of Da Afghanistan Bank.

Annex I- List of Financial Institutions Regulated by Da Afghanistan Bank who shall comply with this Regulation

Name of financial institution	Activity undertaken
Banks	
Money Service Providers	
Foreign Exchange Dealers	
Electronic Money Institutions	
Depository Micro Finance Institutions	
Brokers	
Prepaid card issuing companies	

Annex II- Customer Identification Requirements for Customers

Financial institutions shall obtain the following information and documents from the customers depending on the type of customer.

(1) Natural persons

1. Full name, Father Name including any aliases.
2. Business Name (in case of sole trader).
3. Gender.
4. National Registration Card/Citizen Scrutiny Card/Passport.
5. Permanent and mailing address.
6. Date of birth.
7. Nationality.
8. Occupation.
9. Income and source of income.
10. Phone number (if any).
11. Photo.

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

(2) 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 and email address).
4. Certificate of Incorporation should be updated annually, 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 as paragraph (1)above.”

9. “Identification documents of Settlors, Trustees, Protectors and beneficiaries with respect to trusts as paragraph (1).”

10. Board or any other competent authority’s 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/financial institution.

Financial institutions should verify the authenticity of the information provided by the company/business with the relevant license issuing authority.

For foreign incorporated or foreign registered business entities, comparable documents should be obtained. Banks and financial institutions should 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 Afghanistan.

(3) Non-Government Organization (NGO) and Non-Profit Organizations (NPOs)

1. Name of Non-Government Organization/Non-Profit Organization.
2. Full Address.
3. Certification of registration.
4. Constitution of the NGO/NPO.
5. Name and address of Executive committee.
6. Telephone No. and email address.
7. Executive committee's decision regarding opening of account.
8. Identification documents of directors/senior officers of the NGO/NPO.
9. Authorization for the operation of accounts financial transactions.
10. Identification documents to identify the person authorized to represent the NGO/NPO in its dealings with the bank/financial institution.
11. Copy of the latest certified taxation return and related documentation.
12. Copy of the latest financial statement.

Annex III-Examples High and Low Risk Situations Requiring Enhanced or Simplified Customer Due Diligence

(1) When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas and particular products, services, transactions or delivery channels, financial institutions can have regard to the following potentially higher risk situations that would require the application of enhanced customer due diligence:

1) Customer risk factors:

1. The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer).
2. Non-resident customers.
3. Legal persons or arrangements that manage the assets of third parties.
4. Companies that have nominee shareholders or shares in bearer form.
5. Activities that are cash-intensive or susceptible to money laundering or terrorism financing.
6. The ownership structure of the company appears unusual or excessively complex with no visible economic or lawful purpose given the nature of the company's business.
7. Business relationships and transactions conducted other than "face-to-face".
8. Business relationships conducted in or with countries as identified in Section 11(b) below.
9. Politically exposed persons ("PEP") or customers linked to a PEP.
10. High net worth customers, or customers whose source of income or assets is unclear.
11. Businesses/activities identified by the FIU, Da Afghanistan Bank or the FATF as of higher money laundering or financing of terrorism risk.

2) 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 Da Afghanistan Bank or the FIU 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.

3) Products, services, 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.

(2) When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas and particular products, services, transactions or delivery channels, financial institutions can have regard to the following potentially low risk situations that would require the application of simplified customer due diligence:

1) Customer risk factors

1. Financial institutions and Designated Non-Financial Businesses and Professions – where they are subject to requirements to combat money laundering and terrorism financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements.
2. Companies listed on a stock exchange and subject to disclosure requirements (either by law, or stock exchange rules or other binding Instructions or Regulations), which define requirements to ensure disclosure of beneficial ownership.
3. Public enterprises.

2) Product, service, transaction or delivery channel risk factors:

Financial products or services where there is a proven low risk of money laundering or terrorist financing which occurs in strictly limited and justified circumstances and it relates to a particular type of financial institution or activity or a financial activity is carried out by a natural or legal person on an occasional or very limited basis such that there is a low risk of money laundering and terrorist financing and that are provided to a low risk customer for financial inclusion purposes.

3) Country risk factors:

1. Countries classified by credible sources, such as mutual evaluation reports, as having effective AML/CFT systems.
2. Countries classified by credible sources as having a low level of corruption or other criminal activity.