UNOFFICIAL TRANSLATION

Approved by the Governor of Bank of Mongolia in 21 Jan 2019, by decree No. A-262
Amended by the Governor of Bank of Mongolia in 27 Jan 2021, by decree No.A-31

THE REGULATION OF PREVENTIVE MEASURES ON ANTI-MO NEY LAUNDERING AND COMBATING FINANCING OF TERRORISM

1. GENERAL PROVISION

1.1 This Preventive Measures Regulation details the requirements, procedures, reporting and practices that must be defined and implemented by entities (reporting entities) described in Article 4.1 of the Law on Anti-Money Laundering and Combating the Financing of the Terrorism (the Law) pursuant to the requirements of the Law as well as in accordance with article 5.14 of the Law.

1.2 This regulation is applicable for all reporting entities specified in Article 4.1.1 through Article 4.1.6 of the Law.

1.3 Reporting entities specified in Articles 4.1.7 through 4.1.9 of the Law are enforced to pursue all the obligations set out in this regulation excluding the Article 9 and Article 12.

1.4 Reporting entities are required to develop internal policies, procedures and programs that are consistent with the requirements of this regulation and the Law and any other requirements, regulations, instructions or directives issued by supervisory authorities (the Bank of Mongolia, Financial Information Unit (FIU) and the Financial Regulation Commission (FRC) or other competent authorities referred to Article 19.1 of the Law.

1.5 It is strictly prohibited to establish the bank described in Article 3.1.7 of the Law.

2. MEASURES TO CONDUCT RISK ASSESSMENTS

2.1 The internal monitoring system referred to in Article 14 of the Law shall be reviewed regularly to ensure that it provides an appropriate response to the money laundering (ML)/terrorist financing (TF) risks being faced by the reporting entity, and shall be modified as required to deal with the risks created by new products, services and delivery channels and associated with particular locations or types of customer.

2.2 Reporting entities shall undertake an assessment of their ML and TF risks in order to ensure that they are in a position to understand and manage those risks giving consideration factors such as:

2.2.1 Consumers risk;
2.2.2 products and services risks;
2.2.3 Geographic and regional risks (i.e. countries or domestic areas in which consumers operate or the place origination or destination of the transactions);
2.2.4 Delivery channels risk (i.e. the risks that arise from the channels used to deliver products and services);
2.2.5 The purpose of account or business relationship;

2.2.6 Risks associated with transactions (including the size of deposits or transactions undertaken by a consumer and the frequency of the transaction or duration of the relationship; whether the transaction is outside of the scope of normal transactions conducted by the consumers or whether the transaction originated or is destine for a high risk jurisdiction).

2.3 The risk assessment and any underlying information shall be documented, be kept up-to-date and be readily available for supervisors to review at their request.

2.4 Having performed an assessment of their ML and TF risks reporting entities shall ensure that their AML/CFT policies and procedures reflect those risks and that appropriate measures to manage and mitigate those risks are put in place. This shall include enhanced measures to manage and mitigate high-risk areas.

2.5 Reporting entities, on the basis of the evaluation pursuant to Article 2.2 shall adopt the following measures to manage the risk:

2.5.1 Obtain additional information on the consumer, beneficial owner, beneficiary and transaction where appropriate.
2.5.2 Establish a risk profile on consumers and transactions. The consumer profile should be based upon sufficient knowledge of the consumer (and beneficial owner(s) as applicable), including the consumer's anticipated business with the reporting entity, and where necessary the source of funds and source of wealth of the consumers.
2.5.3 Apply enhanced consumer due diligence to high-risk consumers, products, services and delivery channels, geographic locations.
2.5.4 For customer identified as low risk by the risk assessment specified in 2.2 of this regulation, reporting entities shall consider consistency with the National risk assessment and the sector risk assessment and could apply simplified customer due diligence within the scope specified in article 5.2.1 and 5.2.2 of the Law on Anti-Money Laundering and Combating the Financing of the Terrorism.
2.5.5 Monitor on an ongoing transaction and the relationship with the consumers. Monitoring should include the scrutiny of transactions to ensure that they are being conducted according to the reporting entities' knowledge of the consumers and the consumers risk profile and, where necessary, the source of funds and wealth and should develop internal monitoring system for this purpose.
2.5.6 Adopt other measures as may be prescribed in guidelines by the Bank of Mongolia, FRC, FIU or other competent authorities as referred to in Article 19.1 of the Law.

2.6 The risk assessment undertaken pursuant to Article 2.1 of this regulation shall have regard to the higher risks associated with business relations and transactions referred to in Article 5.8 and 6 of the Law and include but is not limited to the following factors:

2.6.1 Consumer Risk Factors
2.6.1.1 Business relationships conducted in unusual circumstances (for example relationships conducted over long distances);
2.6.1.2 Non-resident consumers;
2.6.1.3 Consumers that are legal persons or arrangements and that operate as personal asset holding vehicles;
2.6.1.4 Consumers that are legal persons that have nominee shareholders, issuer bearer shares or that are part of an unusual or excessively complex ownership structure;
2.6.2 Geographic and Regional Risk Factors

2.6.2.1 Countries identified by credible sources such as mutual evaluation reports or related documents as having inadequate AML/CFT systems;
2.6.2.2 Countries are subject to sanctions, embargoes or similar measures;
2.6.2.3 Countries identified by credible sources as having significant levels of corruption or other criminal activity;
2.6.2.4 Countries or regions identified by credible sources as providing funding or support for terrorist activities, or that have terrorist organizations operating within them.

2.6.3 Product, service, transaction or delivery channels risk factors
2.6.3.1 Private or exclusive banking services;
2.6.3.2 Anonymous transactions, including cash transactions;
2.6.3.3 Non-face-to-face business relationships or transactions;
2.6.3.4 Transactions involving payment from unknown or un-associated third parties.

2.7 Other risk factors associated with the business of the reporting entity that are detected in the course of the risk assessment conducted pursuant to Article 2 of this regulation or that are referred to in the National Risk Assessment.

3. CONSUMER DUE DILIGENCE

3.1 For the purpose of properly implementing the customer due diligence requirements of the Law and these regulations, customer identification and verification shall include the requirements set out in Tables 1 – 3 below. The objective of the identification and verification requirements of the Law is to identify and verify both the customer of the reporting entity, the beneficial owner and any person that has a beneficial interest in the assets of the customer or who, in the case of a legal person or arrangement, owns, controls or has a beneficial interest in its property. Where layered ownership structures are used it will be necessary to identify and verify the components of each layer until the ultimate beneficial owner or controller is identified.

3.2 For natural persons:

Table 1

Information Required	Verification Required[1]
Surname	Citizen's identity card, or passport
Name	Citizen's identity card, or passport
Date of birth	Citizen's identity card or passport
Number of Registry	Citizen's identity card or passport
Address	The way to receive and verify this information should be regulated in internal control policy.
Employment particulars or information about business:	The way to receive and verify this information should be regulated in internal control policy.

[1] The original, or a certified copy of the record referred to in column 1 of the table shall be viewed by a representative of the reporting entity in accordance with article 5.2.1 of the Law. A copy of the document should be kept as part of the customer file maintained by the reporting entity.

1. To identify business type and scope of business, 2. To identify address of office and position of customer.	
To verify whether they are acting on their own behalf or on behalf of some other person	a) If the customer is acting on behalf of another person, all the information required in table 1, should be obtained in relation to that person or legal entity and verified. b) If the customer is acting on behalf of a legal entity or a legal arrangement the information required in Table 2 or 3 (as required) should be obtained until the ultimate beneficial owner or controller of the property, the subject of the transaction is identified and verified. If the beneficiary owner is uncertain, all required information are subject to be obtained until the direction of person or final decision maker. c) If the customer is acting on behalf a trust, the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership); d) for other types of legal arrangements, the identity of persons in equivalent or similar positions.

3.3 For legal entities:

Table 2	
Information Required	**Verification Required**
Name	Formation documents issued by the company registry at which the legal entity is registered
Registered address	Registration documents issued by the company registry at which the legal entity is registered
Registration number	Registration documents issued by the company registry at which the legal entity is registered
Ownership structure	Share certificates or company returns filed at the company registry at which the legal entity is registered

Business type	Registration documents issued by the company registry at which the legal entity is registered
Directors/office bearers	Registration documents issued by the company registry at which the legal entity is registered or the orders of committee of the shareholders.
Official address or registered phone books	Reporting entities are required to establish their own internal system to obtain this information.
The identity of the natural person or persons for whose benefit the assets of the company are held or who exercise control over the assets of the company[2]	If this person or persons are not a shareholder or office bearer in the legal entity full particulars of the person or persons as required in Table 1 should be obtained, together with the documentation that establishes the entitlement of that person to a beneficial interest in the assets of the company

3.4 If the customer represents or is acting on behalf of a legal arrangement:

Table 3	
Information Required	**Verification Required**
If the customer is a natural person: the information required in Table 1	The verification required for natural persons in Table 1
If the customer is a legal entity: the information required in Table 2	The verification required for legal entities in Table 2
Full particulars of the nature of the legal arrangement, including the name, address and registration details (if any) of (i) any person or entity with the authority to hold or deal in property held pursuant to the legal arrangement; (ii) any person or entity with powers to appoint or dismiss trustees or other persons responsible for implementing the legal arrangement and (iii) any person entitled to receive the benefit of property held by the legal arrangement; and iv) the settlor, the trustee(s), the protector (if any), (v) the beneficiaries or class of beneficiaries;, and (vi) any other natural person exercising ultimate effective control over the trust	Trust deeds or other documents that establish the legal arrangement, set out its powers and identify the beneficiaries. Where persons or legal entities are identified the verification required in either Table 1 or Table 2 should be completed as appropriate.

[2] This information is not required for legal persons that are registered as public companies on the Mongolian Stock Exchange or a foreign stock exchange.

(including through a chain of control/ownership.	

3.5 Reporting entities shall conduct ongoing due diligence and shall gather and maintain customer and beneficial owner 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 reporting entity, for example when:

3.5.1 A significant transaction is to take place;
3.5.2 There is a material change in the way the account is operated;
3.5.3 Information held on the customer is insufficient to enable the reporting entity to understand the nature of the financial relationship or transactions being conducted.

3.6 Where a customer provides false or fictitious information to a reporting entity in the course of the CDD process the reporting entity shall make a suspicious transaction report to the FIU.

3.7 Where a reporting entity is unable to verify the identity of the customer and beneficial owner(s) or comply with other CDD measures set out in the Law or in this Regulations, it shall refrain from opening the account or commencing the business relationship or carrying out the transaction, or it shall terminate the business relationship. In such cases, the reporting entity shall consider filing a suspicious transaction report to the FIU. A reporting entity should also consider submitting a suspicious transaction report to the Financial Information Unit when the customer refuses to provide information required by the law and this Regulation.

3.8 Reporting entities are shall not open accounts, conduct transactions or provide any financial services to individuals or entities designated by the UN or domestic competent authorities as terrorist or a terrorist organization or other individual or entity designated pursuant to laws or regulations relating to the proliferation of weapons of mass destruction or its financing (PF) or as requested by a foreign country. The name of costumers is matched with any of the followings shall take immediate actions described in Article 14 of this regulations.

3.8.1.1 the name of individuals or entities designated as terrorist, terrorist organization pursuant law and regulation;
3.8.1.2 the name of individuals or entities designated pursuant to laws, regulations relating to proliferation of weapons of mass destruction or its financing;

3.9 If the name of customers are matches with any of the names described in Article 3.8, reporting entities shall immediately freeze transactions, accounts, funds and properties, and submit a STR to the FIU within 24 hours.

CDD for beneficiaries of life insurance policies

3.10 For life or other investment-related insurance business, a reporting entity should, in addition to the CDD measures required for the customer and the beneficial owner, conduct the following CDD measures on the beneficiary of life insurance and other investment related insurance policies, as soon as the beneficiary or beneficiaries are identified/designated:

3.10.1 For beneficiary(ies) that are identified as specifically named natural or legal persons or legal arrangements – taking the name of the person;
3.10.2 For beneficiary(ies) that are designated by characteristics or by class (e.g. spouse or children at the time that the insured event occurs) or by other means (e.g. under a will) – obtaining sufficient information concerning the beneficiary to satisfy the

financial institution that it will be able to establish the identity of the beneficiary at the time of the pay-out.

3.10.3 For both the cases referred to in 6.1 (a) and (b) above, the verification of the identity of the beneficiary should occur at the time of the pay-out.

3.11 The beneficiary of a life insurance policy should be included as a relevant risk factor by the reporting entity in determining whether enhanced CDD measures are applicable. If the reporting entity determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, then the enhanced CDD measures should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of a pay-out.

3.12 Where a reporting entity is unable to comply with this Article above, it should consider making a suspicious transaction report.

4. DETERMINATION OF BENEFICIAL OWNERSHIP

4.1 Reporting entities must take reasonable measures to determine if a customer is acting on his/her own or on behalf of one or more beneficial owners. If so, reporting entities should take reasonable steps to verify the identity of the beneficial owner or any person that has a beneficial interest in the assets of the customer or who, in the case of a legal person or arrangement, owns, controls or has a beneficial interest in its property. by using relevant information or data obtained from a reliable source such that the reporting entity is satisfied that it knows the identity of the beneficial owner. The information to be obtained on a beneficial owner should be consistent with the requirements outlined in Tables 1, 2 and 3 of this Regulation or other regulations or guidelines issued.

4.2 For public companies (or other legal persons or legal arrangements) quoted on an exchange regulated by law, and certain non-resident public companies subject to adequate regulatory disclosure requirements and quoted on a foreign exchange licensed by an appropriate regulatory authority that is subject to adequate supervision in a jurisdiction that is implementing effectively the international standards on AML/CFT, no further identification is necessary provided that the reporting entity obtains customer identification documents as outlined in Tables 1, 2 and 3 of this Regulation. In determining if there has been effective implementation in the jurisdiction, reporting entities should take into account the information available on whether these countries adequately apply the international standards on AML/CFT, including by examining the reports and reviews prepared by the Financial Action Task Force (FATF), FATF style regional bodies such as the Asia/Pacific Group on Money Laundering (APG), International Monetary Fund, and World Bank publications.

4.3 Reporting entity shall follow steps described in Article 4 of the Law to determine the beneficial ownership. Meaning of the majority holder described in Article 4.1.1 of the Law shall apply to as directly or indirectly owned 33 percent or more of the total shares.

4.4 For customers that are legal arrangements, reporting entities should be required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

(i) Settlor;
(ii) Trustee(s);
(iii) Beneficiary or class of beneficiaries;
(iv) Protector (if any);
(v) For other types of legal arrangements, the identity of persons in equivalent or similar positions

4.5 In determining indirect ownership of equity interests:

4.5.1 an equity interest held by a company, limited partnership, or similar arrangement and by a trust should be considered as being owned proportionately by its shareholders, partners, or vested beneficiaries; and

4.5.2 an equity interest held by a family member should be considered as also being owned, in its entirety, by each family member.

5. SIMPLIFIED CUSTOMER DUE DILIGENCE

5.1 Possible simplified CDD measures could include, but are not limited to the following:

5.1.1 Reducing the frequency of customer identification updates.

5.1.2 Reducing the degree of on-going monitoring and scrutinizing of transactions.

5.2 Reporting entities 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 identified as high risk by either the reporting entity or either the supervisory authority or FIU.

6. POLITICALLY EXPOSED PERSONS

6.1 Internal controls of a reporting entity specified in article 14 of AML/CFT Law and in article 3 of this Regulations should include a requirement that reporting entities identify PEP's, their family members, associates and parties with common interests. All these persons should be subject to enhanced CDD procedure and transactions on their name should be subject to enhanced monitoring.

6.2 Reporting entity is required to conduct the same measures for customers whose beneficial owner is identified as a politically exposed person.

6.3 Requirements relating to politically exposed persons shall also be applied to persons who are family members or close associates of the politically exposed person.

6.4 In relation to life insurance policies, reporting entities should be required to take reasonable measures to determine whether the beneficiaries and/or, where required, the beneficial owner of the beneficiary, are PEPs. This should occur, at the latest, at the time of the payout. Where higher risks are identified, reporting entities should be required to inform senior management before the payout of the policy proceeds, to conduct enhanced scrutiny on the whole business relationship with the policyholder, and to consider making a suspicious transaction report.

6.5 Reporting entities should also comply with any Regulations or Guidelines issued in relation to PEPs by competent supervisory authority described in Article 19 of the Law.

7. ENHANCED CUSTOMER DUE DILIGENCE

7.1 Reporting entities shall apply enhanced customer due diligence (enhanced CDD) measures to high risk areas:

7.1.1 Identified in the risk assessment undertaken by the reporting entity pursuant to article 14 of the Law, Mongolia's National risk assessment and article 2 of the Regulation; and

7.1.2 Referred to in article 2 of the regulation.

7.2 Reporting entities shall consider the following as a high risk:

7.2.1 Customers referred to in Article 5.9 of the Law;

7.2.2 Transactions referred to in Article 6 of the Law;

7.2.3 Transactions associated with countries or geographic regions that are identified as being a high money laundering or terrorist financing risk by the FIU or a supervisor or international organizations including the Financial Action Task Force and the Asia Pacific Group on Money Laundering or other similar regional body;

7.2.4 Transactions involving wire transfers, politically exposed persons (whether as customer or beneficial owner) or through correspondent arrangements;

7.2.5 Transactions with non-face-to-face customers or where customer due diligence (CDD) has been undertaken by a third-party intermediary.

7.3 Enhanced CDD shall be applied to customers and transactions that are high risk.

7.4 The FIU or the supervisory authorities may impose counter measures to transactions associates with countries or geographic regions that are identified as being a high ML or TF risk by the FIU or the supervisory authority or international organizations including the Financial Action Task Force and the Asia Pacific Group on Money Laundering or other similar regional body. The counter measures that may be imposed by the FIU or the supervisory authority include, but are not limited to:

7.4.1 Requiring reporting entities to apply specific elements of enhanced due diligence;

7.4.2 Introducing enhanced relevant reporting mechanisms or systematic reporting of financial transactions

7.4.3 Refusing the establishment of subsidiaries or branches or representative offices of financial institutions from the country concerned, or otherwise taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems

7.4.4 Prohibiting reporting entities from establishing branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant branch or representative office would be in a country that does not have adequate AML/CFT systems.

7.4.5 Limiting business relationships or financial transactions with the identified country or persons from that country.

7.4.6 Prohibiting reporting entities from relying on third parties located in the country concerned to conduct elements of the CDD process.

7.4.7 Requiring reporting entities to review and amend, or if necessary terminate, correspondent relationships with financial institutions in the country concerned.

7.4.8 Requiring increased supervisory examination and/or external audit requirements for branches and subsidiaries of financial institutions in the country concerned.

7.4.9 Requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned

7.5 Enhanced CDD should include, but is not limited to, the following:

7.5.1 Obtaining additional information from the customer relating to the customer's business, source of funds, the purpose of intended transactions and, where possible, verifying such information;

7.5.2 Obtaining the approval of senior management for continuation of the business relationship with the customer. This approval process should take place in the context of appropriate customer acceptance policies that include refusal of acceptance of business with customers who pose an excessively high ML/TF risk;

7.5.3 the conduct of higher level (frequency and depth) monitoring of the customer's transactions and review of CDD requirements;

7.5.4 other requirements relating to enhanced CDD that may be the subject of regulations pursuant to Article 5.3 of the Law approved by the Governor of the Bank of Mongolia or pursuant to Article 19.2.3 of the Law approved by either the Bank of Mongolia or the Financial Regulatory Commission.

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

8. THIRD PARTY INTRODUCERS

8.1 Reporting entities may rely on third parties to undertake customer due diligence procedures related to identification of the customer, beneficial ownership and understanding the nature of the business. The ultimate responsibility for customer identification and verification shall remain with the reporting entity relying on the third party.

8.2 Where a reporting entity uses a third party to undertake customer due diligence procedures on its behalf it should ensure that all information that has been obtained by the third party is sent to it as soon as practicable and that copies of documents obtained as part of the customer due diligence process are either provided or can be obtained immediately upon request.

8.3 Arrangements with third party introducers should be documented and available for review by the supervisory authority, upon request.

8.4 Prior to entering into a relationship with a third party, reporting entities should have regard to the money laundering and terrorist financing risk associated with the country in which the third party is based.

8.5 Reporting entities should ensure that any third party used by it for customer due diligence procedures is:

8.5.1 Subject to AML/CFT regulation, supervision or monitoring;
8.5.2 Has customer due diligence procedures in place that are consistent with the requirements of the Law and these regulations; and
8.5.3 Subject to record keeping requirements that are consistent with those of the Law.

8.6 For financial institutions that rely on a third party that is part of the same financial group, supervisors may also consider that the requirements of the criteria above are met in the following circumstances:

8.6.1 the group applies CDD and record-keeping requirements and programmes against money laundering and terrorist financing, in accordance with the Law and Regulations 18;
8.6.2 the implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent supervisory authority; and
8.6.3 any higher country risk is adequately mitigated by the group's AML/CFT policies.

9. CORRESPONDENT BANKING RELATIONSHIPS

9.1 Before establishing cross-border correspondent arrangements and similar relationships, reporting entities shall:

9.1.1 to obtain information whether this bank exists,
9.1.2 based on publicly-available information, evaluate the respondent institution's reputation and the nature and quality of supervision to which it is subject and whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;
9.1.3 obtain approval from senior management before establishing a correspondent relationship;
9.1.4 to evaluate the internal controls implemented by the respondent institution with respect to anti-money laundering and combating the financing of terrorism;
9.1.5 establish an agreement on the respective rights and responsibilities of each party under the relationship;
9.1.6 in the case of a payable-through account, ensure that the respondent institution has undertaken CDD measures, including the verification of its customer's identity, has implemented mechanisms for ongoing monitoring with respect to its customers, and is capable of providing and shall provide relevant CDD information on request.

9.2 A reporting entity shall not establish correspondent relationship with shell bank and financial institution.

9.3 A reporting entity shall not establish or continue business relations with a respondent financial institution in a foreign country if the respondent institution permits its accounts to be used by a shell bank.

9.4 Reporting entities should review existing correspondent relationships to meet requirements stated in this regulation.

10. NEW TECHNOLOGIES

10.1 The measures that should be implemented to reduce the risks associated with the use of new or developing technologies referred to in article 5.8 of the AML/CFT Law should include:
10.1.1 Prior to introducing new products, services or delivery mechanisms, reporting entities should undertake an assessment of the risks associated with such products, services and delivery mechanisms, and undertake an assessment of the risks associated with the use of new or developing technologies with both new or pre-existing products; and
10.1.2 Implementing appropriate measures designed to manage such risks and mitigate those risks.

11. INTERNAL CONTROL AND PROCEDURES

11.1 The internal policies, procedures, systems and controls should be consistent with the reporting entities' size, nature, risks, and complexity of operations and should be adopted by the entities' board of directors and be applicable to all domestic and foreign branches and majority-owned subsidiaries of the entity.

11.2 The internal policies, procedures, internal controls stated in 11.2.1 should be consistent with the reporting entities' size, nature, risk, and structure but must be sufficient and effective to deal with ML/FT risk. The internal policies, procedures, internal controls should be applicable to all domestic and foreign branches and majority owned subsidiaries of the entity.

11.3 Board, relative committees or Internal audit committee of reporting entity shall review implementation of the internal policies, procedures regularly and ensure that internal policies, procedures are sufficient and effective to deal with AML/CFT risk and update it, if necessary.

11.4 The internal control system referred to in Article 14 of the Law shall also contain the following components:

11.4.1 A specified AML/CFT training program for activities identified as higher risk activities;

11.4.2 written procedures and manuals guiding staff on the operation of the reporting entities' AML/CFT systems and controls;

11.4.3 Procedures for the appointment of a compliance officer and the creation of a compliance unit (if required) and policies relating to the compliance officers' power and responsibilities and reporting duties. The Compliance officer should be senior level staff;

11.4.4 The Compliance officer should have access and right to have all documents and information from subsidiaries, units, branches related to customer account and transactions;

11.4.5 Reporting entities must establish and maintain an adequately resourced and independent audit function. The independent audit function shall be responsible to test the AML/CFT system and to ensure that the compliance officer and staff of reporting entity are performing their duties in accordance with the reporting entities' AML/CFT internal policies, procedures, systems and control;

11.4.6 Reporting entities must establish screening procedures to ensure appropriate standards when hiring employees. Employee screening procedures must ensure that:

- employees have the high level of competence necessary for performing their duties;
- employees have appropriate ability and integrity to conduct the business activities of the bank or financial institutions;
- potential conflicts of interests are taken into account, including the financial background of the employee;
- fit and proper and code of conduct requirements are defined;
- persons charged or convicted of offences involving fraud, money laundering, and other financial crimes, dishonesty or other similar offences are not employed by the reporting entity.

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

(i) all suspicious transactions detected, and implications for the reporting entity,

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

(iii) results of any onsite inspections conducted by the supervisory authority or FIU,

(iv) statement on remedial actions required to be implemented by the reporting entity.

12. WIRE TRANSFERS

12.1 Reporting entities that engage in cross border wire transfers shall include accurate originator and recipient 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:

12.1.1 The full name of the originator;

12.1.2 The originator account number where such an account is used to process the transaction;

12.1.3 The originator's address, or national identity number, or customer identification number, or date and place of birth;

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

12.2 In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.

12.3 Where several individual cross-border wire transfers from a single originator are bundled in a batch transfer for transmission to beneficiaries, reporting entities are not required to apply the provisions of Article 12.1 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 transfer contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

12.4 Reporting entities should ensure that non-routine wire transfers are not batched where this would increase the risk of money laundering or terrorism financing.

12.5 For domestic wire transfers (including transactions using a credit or debit card as a payment system to effect a money transfer), the ordering reporting entity must include either:

12.5.1 full originator information in the message or payment form accompanying the wire transfer; or

12.5.2 only the originator's account number, where no account number exists, a unique identifier, within the message or payment form.

12.6 Where full originator information has not been included in a domestic wire transfer, this information should be made available by the ordering reporting entity within three business days of receiving the request either from the beneficiary financial institution or from the Financial Intelligence Unit.

12.7 For cross-border wire transfers, reporting entities processing an intermediary element of the payment chain should keep all wire transfer information including originator and beneficiary information for at least 5 years.

12.8 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 reporting entity should keep a record, for at least five years, of all the information received from the ordering or other intermediary institution.

12.9 Reporting entities should have effective risk-based procedures for determining:

12.9.1 when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information and considering reporting to the Financial Information Unit;

12.9.2 the appropriate follow-up action which may include restricting or terminating business relationships.

12.10 For wire transfers, a beneficiary reporting entity 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 the Law.

Intermediary financial institutions

12.11 For cross-border wire transfers, an intermediary financial institution must ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it.

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

12.13 Intermediary financial institutions should take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack required originator information or required beneficiary information.

12.14 Intermediary financial institutions should have risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action.

Beneficiary financial institutions

12.15 Beneficiary financial institutions must take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack required originator information or required beneficiary information.

12.16 For cross-border wire transfers, a beneficiary financial institution must verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with the record keeping provisions of the Law and this Regulation.

12.17 Beneficiary financial institutions should have risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action.

12.18 Money or value transfer service (MVTS) providers including their agents, that are not entities described under Article 4.1.1 of the Law are required to comply with all of the relevant requirements of Article 12 of this Regulations.

12.19 If money or value transfer service providers using external agents, they shall register to FRC in perspective of its requirements and the agents shall be obliged to implement the internal procedures of the MVSP. Money or value transfer service providers shall monitor the agent's activity on the implication of AML/CFT.

12.20 In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider:

12.20.1 should take into account all the information from both the ordering and beneficiary sides in order to determine whether a STR has to be submitted to the FIU; and

12.20.2 should file a STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit.

12.21 If the reporting entity is unable to comply with these requirements, it shall not execute the wire transfer.

13. OBLIGATIONS OF TRUSTEES

13.1 A trustee shall disclose its status to a reporting entity, when as a trustee, before it establishes a business relationship or carries out an occasional transaction above the threshold set out in Article 7.1 of the Law.

13.2 A Trustee shall provide reporting entities with information on the beneficial ownership and the assets of the trust to be held or managed under the terms of the business relationship.

14. TARGETED FINANCIAL SANCTIONS

14.1 Reporting entities obliged to implement targeted financial sanctions which is approved by the Government associated with the proliferation of weapons of mass destruction and the combating terrorism, based on the United Nations Security Council Resolutions and decision of national organization in charge of combating terrorism, against person and legal entities, pursuant to article 6^1 of the Law on Anti-Money Laundering and Combating the Financing of the Terrorism, article 23 of the Law on Counter Terrorism and Proliferation of Weapons of Mass Destruction and "Regulations on Targeted Financial Sanctions for the Counter Terrorism and Proliferation of Weapons of Mass Destruction" approved by the annex to the Resolution No. 464 of the Government of Mongolia in 2019.

14.2 When General Intelligence Agency and National Counter Terrorism Council promptly informs the list to the relevant supervisory authority to reporting entities and public and publishes it in their website www.gia.gov.m; www.nctc.gov.mn, reporting entity shall conduct a search of its records to determine whether the entity has any customer, transaction, contract, agreement, asset and fund that are directly or indirectly related to the persons or legal entities /hereinafter referred to as "listed persons, legal entities"/ included in the targeted financial sanctions list and domestic list.

14.3 If reporting entity considers that they have assets or funds directly or indirectly relevant or guided activities with persons, legal entities in the list or behalf of them, the reporting entity obliged to apply procedures pursuant to article 6^1.2 of Law on Anti-Money Laundering and Combating the Financing of the Terrorism and article 23.6 and 24 of Law on Counter Terrorism and Proliferation of Weapons of Mass Destruction.

14.4 To implement its obligation set out in article 14.3 of this regulation, a reporting entity shall provide the information specified in appendix No.5 as Form 5 /Assets report of listed persons and legal entities/ of "Methodology for Implementing Targeted Financial Sanctions for the Proliferation of "Standard Operational Procedural Manual for Implementing Targeted Financial Sanctions for Countering Terrorism and Proliferation of Weapons of Mass Destruction" approved by Decree A/34 of the Director General of the General Intelligence Agency in 2020, to the General Intelligence Agency and the Financial Intelligence Unit.

14.5 Reporting entities submit inquiries formed as appendix No.6 as Form 6/verification assistance form/ to the General Intelligence agency, if they have needs to verify person, legal entities in the list for the implementation of their obligation set out in article 14.3 of this regulation.

14.6 Reporting entities submit a request for reimbursement of necessary expenses, certain type of fees, service fees and contingencies by frozen assets in accordance with appendix form No.7 as Form 7 /Form requesting permission to provide assets and financial services to listed person, legal entity/ of the methodology specified 14.4 of this regulation, to the General Intelligence Agency.

14.7 Reporting entity shall have a legal and organizational system, which is based on recommendation of UN Security council and domestic competent authorities in regard of AML/CFT and Proliferation, fits in the implementation of target financial sanctions against individuals and legal entities approved by Government in connection with the proliferation of weapons of mass destruction and terrorism:

14.7.1 Shall have a procedure to search in its data base whether listed persons or legal entity's any assets or money is placed and to inform the General Intelligence Agency about the outcomes.

14.7.2 Shall have an internal regulation on the activities of detecting and immediately freezing the assets of listed persons and legal entities and informing the General Intelligence Agency and FIU.

14.7.3 Shall have an internal regulation on controlling and restricting attempts of customers and other persons to access the assets of listed persons and legal entities.

14.7.4 Shall have an internal regulation, which is based on the directions and suggestion by the General Intelligence Agency, on providing the financial services can be given to listed persons or legal entity.

14.7.5 Shall have an internal regulation on implementing the decision to release the assets of persons or legal entities in the list submitted by the General Intelligence Agency.

14.8 Reporting entity must report the implementation of target financial sanctions against individuals and legal entities approved by Government in connection with the proliferation of weapons of mass destruction and fight against terrorism to domestic competent authority in regard of inspection. This shall be based on recommendation of UN Security council and domestic competent authorities in regard of AML/CFT and Proliferation.

15. RECORD KEEPING

15.1 For the purposes of complying with article 8 of the AML/CFT Law reporting entities shall retain records as follows:

Table 4

Type of Record	Retention Period
Records relating to the establishment of a customer relationship including account opening documents and documents relating to KYC procedures, including copies of identification documents	5 years after the customer relationship has ended, or where such documents have arisen from an occasional transaction, 5 years from that transaction
Records and documents relating to enhanced CDD procedure. The updates of customers' information additional information, documents, information about accounts. Agreement on correspondence relationship, memorandum, and records used to identify ML/TF risk, documents on analysis of ongoing CDD, analysis of enhanced monitoring of transactions, information and documents relating to suspicious transactions reports.	5 years after the customer relationship has ended
Records relating to cash or non-cash transactions	5 years from the date of completion of the transaction

15.2 Records that are required to be retained pursuant to the AML/CFT Law and these regulations should be sufficiently detailed to permit the reconstruction of each individual transaction and to enable them to comply swiftly with information requests from the competent authorities stated in the Law.

15.3 Records should be archived to meet all the requirements and consistent with evidence rules.

16. FOREIGN BRANCHES AND MAJORITY OWNED SUBSIDIRIES

16.1 Reporting entities shall require their foreign branches (if any) and majority-owned subsidiaries to implement the requirements of the Law and Regulation to the extent that applicable laws and regulations in the country where the foreign branch or majority owned subsidiaries are domiciled so permit. If such laws prevent compliance with these obligations for any reason, the reporting entity shall so report its supervisor, which may take such steps as it believes to be appropriate to accomplish the purpose of the Act and this Regulation and the financial groups shall apply appropriate additional measures to manage the ML/TF risks.

16.2 Financial groups are required to implement group-wide programs against ML/TF, which should be applicable, and appropriate to, all branches and majority-owned subsidiaries of the financial group. These should include the measures set out in Article 11 of this Regulation and Article 14 of the Law and the following:

16.2.1 Policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management and the implementation of the STR regime;
16.2.2 The provision, at group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes; and
16.2.3 Adequate safeguards on the confidentiality and use of information exchanged.

17. SECTOR SPECIFIC INSTRUCTIONS

17.1 For purpose of assisting with compliance with the law on AML/CFT and this regulation, a supervisor may issue specific instructions to the type or sector of reporting entities that they regulate.

18. REPORTING TRANSACTIONS

18.1 The Reporting entity is responsible for reporting Cash and non-cash transactions of 20 million togrog (or equivalent foreign currency) or above to the Financial Information Unit in the prescribed form within 5 working days.

18.2 The Reporting entities shall report to the Financial Information Unit any transactions that they suspect of money laundering or terrorism financing in prescribed form within 24 hours.

18.3 Reporting entity shall submit the information specified in articles 13 and 14 of the law on Proliferation of weapons of mass destruction and terrorism in electronic form to the FIU in accordance with article 7.3 of the law on Anti-Money laundering and combating the finance of the Terrorism.

18.4 The Reporting entity is obliged to maintain the safety of the person responsible for reporting suspicious transactions and secrecy of the information.

18.5 Each quarter, the FIU will publish on its website and the website of the Central Bank the statistics of STR's, CTR's and FSTR's receive.

18.6 Where there is suspicion of money laundering or terrorist financing, a report shall be made regardless of any threshold or exemption.

18.7 Reporting entity shall summit all available holding relevant documents and additional information related to the suspicious transaction to FIU together with STR.

19. TIPPING OFF AND PROTECTIONS

19.1 Reporting entities, their directors, officers and employees are prohibited from disclosing to a customer or any other person the fact that a report under the law and this Regulation, any Supplementary Information or any information related to the Financial Information Unit or to any money laundering or terrorism financing investigation has been submitted to the FIU. This shall not preclude disclosures or communications between and among directors and employees of the reporting entities, in addition to lawyers, competent authorities, and the Public Prosecution Service.

19.2 In accordance with the Law it is prohibited to disclose information to a person or a legal entity other than authorized officials of authorities and information pertaining to the suspension of transactions or the freezing of accounts, transaction, account.

19.3 No criminal, civil, or administrative proceedings for breach of banking or professional secrecy or contract shall lie against reporting entities 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 and this Regulation

19.4 Notwithstanding any provisions relating secrecy and confidentiality, a reporting entity shall be able to share information with other reporting entities, supervisors and other competent authorities for purposes of complying with the law and this regulation.

19.5 Without limiting the generality of Article 19.4, a reporting entity shall be able to share information when implementing provisions relating to correspondent banking, wire transfers, reliance on third parties and when sharing information pursuant to the requirements of the law and this regulation.

20. RESPONSIBILTY

20.1 Any person who violates the provisions of this regulation shall be penalized according to relevant law and regulation.

____o0o____