

Republic of the Union of Myanmar

Office of the President

Anti-Money Laundering Order

Order No. 45 / 2019

3<sup>rd</sup> Waning of Tazaungmon, 1381 ME

(14 November 2019)

1. This order shall be called the Anti-Money Laundering Order.
2. The following expressions contained in this order shall have the meanings given hereunder:

(a) **Banks and financial institutions** mean banks and financial institutions established by the Myanmar Financial Institutions Law and other relevant laws. This expression includes commercial banks or development banks, credit societies, finance companies, securities exchange companies, money changers, microfinance institutions, insurance companies and other institutions that conduct one or more of the following activities as a business for or on behalf of a customer, including:

- (1) Activities included under the Banks and Financial Institutions definition stated in the Anti-Money Laundering Law
- (2) Financial Leasing
- (3) Keeping safe deposit boxes, safe keeping of cash and managing cash or liquid securities on behalf of other persons.

(b) **Physical presence** means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.

(c) **Legal persons** mean any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This expression also includes companies, corporations, joint ventures, bodies corporate, foundations, anstalt,



partnerships, or associations, organizations of a group of persons and other relevantly similar entities..

- (d) **Legal arrangements** refer to express trusts or other similar legal arrangements.
- (e) **Beneficial ownership** is defined as per the definition included in the Anti-Money Laundering Law. This expression also includes the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.
- (f) **Ultimate effective control** means a situation in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.
- (g) **Customer** means the same as the expression defined in the Anti-Money Laundering Law. This expression also includes any person who has a business relationship with a Reporting Organization.
- (h) **Property** means the same as the expression defined in the Anti-Money Laundering Law. This expression includes property of every kind, whether intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including but not limited to, bank credits, travelers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets .
- (i) **Proceeds of Crime or Money and property obtained by illegal means** means the same as the expression defined in the Anti-Money Laundering



Law. This expression also includes economic gains including income or other benefits derived from such proceeds from property and property converted or transformed, in whole or in part, into another property.

- (j) **Negotiable instrument** means the same as the expression defined in the Anti-Money Laundering Law. This expression also includes bearer negotiable instruments. Bearer negotiable instruments include monetary instruments in bearer form such as: traveler's cheques; negotiable instruments including cheques, promissory notes and money orders that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; and incomplete instruments signed, but with the payee's name omitted.
- (k) **Wire or electronic transfer** means the same as the expression defined in the Anti-Money Laundering Law. This expression also includes any transaction carried out on behalf of an originator through a financial institution by electronic means, with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person. It also includes cross-border and domestic wire or electronic transfers.
- (l) **Cross-border wire or electronic transfer** means any wire or electronic transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire or electronic transfer in which at least one of the financial institutions involved is located in a different country.
- (m) **Domestic wire or electronic transfer** means any wire or electronic transfer where the ordering financial institution and beneficiary financial institution



are located in the same country. This term therefore refers to any chain of wire or electronic transfer that takes place entirely within the borders of a single country, even though the system used to transfer the payment message may be located in another country.

- (n) Designated non-financial businesses and professions mean the same as the expression defined in the Anti-Money Laundering Law. This expression also includes lawyers, notaries, other independent legal professionals and accountants, and sole practitioners, partners or employed professionals within professional firms.

3. The offences referred to in Chapter (3) of the Anti-Money Laundering Law include the following offences:

- (a) offences relating to terrorism and financing of terrorism
- (b) offences relating to trafficking in humans and migrant smuggling
- (c) offences relating to illicit trafficking of narcotic drugs and psychotropic substances
- (d) offences relating to illicit arms trafficking
- (e) offences relating to trafficking of stolen and other illicit goods
- (f) corruption
- (g) fraud
- (h) offences relating to counterfeit money
- (i) offences relating to counterfeit goods
- (j) offences relating to murder or causing grievous bodily harm
- (k) offences relating to kidnapping, illegal restraint and taking hostage
- (l) offences relating to robbery or theft
- (m) offences relating to smuggling
- (n) offences relating to extortion
- (o) offences relating to forgery



- (p) offences relating to converting or transferring any money and property knowing, or having reason to believe, that it is obtained from the commission of any offence, in order to disguise or conceal the source of such money and property, or with the intention of aiding a person involved in a predicate offence or after its commission to avoid the legal consequences of his actions
- (q) concealing or disguising the proceeds of crime of their true nature, source, location, inherent property, conversion or ownership, knowing or having reason to believe that they are obtained from committing an offence
- (r) obtaining, keeping in possession or using such profits, knowing or having reason to believe at the time of receipt that they are the proceeds of crime
- (s) attempting or conspiring, aiding, supporting, facilitating, abetting, providing, recruiting, managing, associating with or counseling the commission of an anti-money laundering offence including the abovementioned offences
- (t) being a member of an organized crime group that commits, attempts to commit or conspires to commit a money-laundering offence including the abovementioned offences
- (u) inciting a person to commit a money-laundering offence, or conspiring with or deliberately facilitating a person or persons to commit money-laundering
- (v) laundering money and property in Myanmar that is derived from committing an offence abroad where the act constitutes an offence in that country and would have constituted any of the abovementioned offences had the same act been committed in Myanmar.

4. The Financial Intelligence Unit referred to in Chapter (5) of the Anti-Money Laundering Law shall be operationally independent and autonomous by:



- (a) having authority and capacity to carry out its functions freely, including the autonomous decision to analyze, request or forward or disseminate specific information
  - (b) being able to make arrangements or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information
  - (c) when it is located within the existing structure of another authority, having distinct core functions from those of the other authority; and
  - (d) being able to obtain and deploy the resources needed to carry out its functions, on an individual or routine basis, free from any undue political, government or industry influence or interference which might compromise its operational independence.
5. The duties of Financial Intelligence Unit referred to in Chapter (5) of the Anti-Money Laundering Law, shall also include the following:
- (a) shall receive, analyze and disseminate suspicious transaction reports submitted by reporting organizations, and other information related to money laundering, financing of terrorism and predicate offences
  - (b) shall conduct operational analysis, which focuses on individual cases and specific targets, activities or transactions, or on appropriate selected information, depending on the type and volume of the disclosures received and the expected use after dissemination
  - (c) shall conduct strategic analysis to deal with the trends and typologies related to money laundering and financing of terrorism
6. The Scrutiny Board described in Chapter (6) of the Anti-Money Laundering Law, shall collaborate with the Bureau of Special Investigations and shall conduct investigations.



7. The Bureau of Special Investigations collaborating with the Scrutiny Board shall have the following duties:

- (a) shall investigate offences related to money laundering and terrorist financing, based on the results of the analysis shared by the Scrutiny Board or the results of the parallel financial investigations on the offences conducted by law enforcement agencies in accordance with the existing laws, or on other sources of information
- (b) may apply interception measures, investigation powers and special investigation techniques as follows
  - (1) investigate, detect, search, seize, freeze or return the money and property under bond
  - (2) to arrange for a bond
  - (3) seal or prohibit the exhibit from being managed or accessed by any other means
  - (4) compel reporting organizations to produce financial records
  - (5) take steps to prevent actions that may affect or obstruct the State's ability to freeze, seize or recover property that is subject to confiscation

8. The Central Body shall issue orders to conduct the following duties not more than (3) months at a time according to the request of the Financial Intelligence Unit and the Bureau of Special Investigations:

- (a) undercover operations
- (b) controlled delivery
- (c) access to bank accounts
- (d) access to computer systems, networks and servers
- (e) place under surveillance or intercept telephone lines, fax machines or electronic transmission or communication facilities

- (f) obtain audio or video files of movements and behaviors or conversations
  - (g) seize information relating to money laundering and financing of terrorism, notarized and private deeds, or banking, financial and business records
9. Witnesses, informants, activists and their family members who give information of money and property with regard to money laundering and terrorist financing shall be protected under the laws, rules, procedures and directives in the following ways;
- (a) Non-disclosure or limitations of the witness's testimony, not to input the witness's testimony in the court record;
  - (b) Non-disclosure or limitations of the identity of the witness;
  - (c) Without the approval of the witness, not to summon the witness to testify in proceeding;
  - (d) Not to use the witness's testimony in any conviction or in fact of decision;
10. Reporting organizations shall be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.
11. The reporting organizations shall immediately report to the Financial Intelligence Unit when the money or property transaction is equal to or exceeds the threshold value.
12. The reporting organizations shall—
- (a) conduct the following due diligence at appropriate times as prescribed under this order, on accounts and customers that existed prior to the enactment of the Law and the new ones, based on the products, services and their risk:
    - (1) conduct due diligence measures when the risk of money laundering and terrorist financing is identified as high risk of money laundering as a result of the risk assessment, conducting enhanced customer due diligence measures consistent with the identified risk, and



determining whether or not the transactions or other activities are unusual or suspicious;

- (2) conduct simplified due diligence measures consistent with the level of risk, if the customer is identified as low risk according to the risk assessment of money laundering or terrorist financing;
  - (3) terminating simplified due diligence measures on the customer under above sub-article (2) if the customer is suspected of money laundering or terrorist financing, or identified as high risk;
  - (4) conduct enhanced due diligence and simplified due diligence measures on the customer in accordance with the directives of the competent authority.
- (b) Due diligence measures on the customer referred to in sub-article (a) shall be conducted under the following times and situations:
- (1) before carrying out transactions for a customer, or before opening an account or establishing a relationship;
  - (2) before carrying out a transaction for a customer who has no established relationship with the reporting organization, if the transaction is equal to or above the threshold amount of USD 15000 or equivalent amount in any currency or as from time to time defined by the Central Body, whether conducted as a single transaction or several connected transactions;
  - (3) before carrying out a domestic and international wire or electronic transfer for a customer;
  - (4) when there is doubt about the veracity or adequacy of the customer identification data obtained previously;
  - (5) when there is suspicion that it is linked to money laundering or terrorist financing



- (c) If the value of transactions referred to in sub-article (b) is unknown at the time of operation, verification and identification in accordance with the provisions of sub-article (a) of such amount shall be made as soon as it is made known, or as soon as it has reached the threshold amount.
- (d) Customer due diligence measures under sub-article (a) shall be under - taken as follows:
  - (1) Identifying and verifying the customer's identity using independent and reliable independent sources, documents, data or information;
  - (2) collecting information on and understanding the purpose and intended nature of the business relationship;
  - (3) identifying the beneficial owner and taking all reasonable measures to verify the identity of the beneficial owner, and understanding the ownership and control structure of the company formation or legal person or legal arrangement,
  - (4) verify if a person acting on behalf of a person, company, organization or legal person or legal arrangements is so authorized, the authenticity of his identity and the legal status of the company, organization or legal arrangement; obtain information on the customer's name, legal structure, address, details of the directors; and specify Regulations that will have binding on the company or legal person or legal arrangements.

13. In the conduct of investigation into money laundering associated predicate offences, financing of terrorism offence, the relevant law enforcement agency can request for all relevant information held by the Financial Intelligent Unit, in accordance with the provisions the Anti-money Laundering Law.

14. According to sub-section (d), section 19, Chapter (8) of Anti-Money Laundering Law, the reporting organizations shall conduct due diligence base on beneficial owners



of the customer and take reasonable measures to verify the identity of such persons, based on the following information:

(a) For legal person

- (1) identity of the natural persons if any– as ownership interest can be so diversified that there are non–natural persons whether acting alone or together exercising control of the legal person or arrangement through ownership who ultimately have a controlling ownership interest in a legal person.
- (2) to the extent that there is doubt under above sub–article (a–1) as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where non–natural person exerts control through ownership interests, the identity of the natural persons if any exercising control of the legal person or arrangement through other means
- (3) Where non–natural person is identified under above sub–article (a–1) or (a–2), financial institutions should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official.

(b) For legal arrangements

- (1) Trusts – the identify 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,
- (2) Other types of legal arrangements – the identity of persons in equivalent or similar positions.



15. If the reporting organizations have formed a suspicion of ML or TF, and if they reasonably believe that performing the CDD process will tip-off the customer, they can stop pursuing the CDD process, and instead submit a STR to the FIU.

16. Reporting organizations shall have appropriate risk management systems to determine whether a customer or a beneficial owner is a domestic or foreign politically exposed person or international politically exposed person, and carry them out as follows:

a. With respect to foreign politically exposed persons–

(1) seeking prior consent from senior management before establishing or continuing a business relationship;

(2) taking all appropriate measures to identify the wealth and source of funds;

(3) applying enhanced on-going due diligence measures on the customer and monitoring such business relationships;

b. applying measures contained in sub-article (a) if the domestic and international politically exposed persons are determined to be high risk.

17. Reporting organizations shall conduct customer due diligence measures with respect to domestic or foreign politically exposed person or international politically exposed person as referred to in the section 22, Chapter (8) of the Anti-Money Laundering Law. The requirements for all types of politically exposed persons shall be applied to their family members and close associates.

18. Reporting organizations shall identify and assess money laundering and terrorist financing risks that arise from new and existing products, services, commercial activities or technologies, including delivery channels, and take necessary action to manage and mitigate such risks. In the case of new products, services, technologies and delivery channels the risk assessment should take prior to the launch of the new products, business practices or the use of new or developing technologies.

19. The bank or financial institution shall carry out the following in addition to performing normal customer due diligence measures contained in section 12 before entering into cross-border correspondent banking and other similar relationships:

- (a) Collecting sufficient information about the respondent institution to understand the nature of its business, and determine from publicly available information its reputation, whether it has been investigated or subject to sanctions relating to money laundering or the financing of terrorism and the quality of its supervision;
- (b) obtaining approval from senior management;
- (c) conducting an assessment of the quality of anti-money laundering and countering the financing of terrorism controls of the respondent institution; and
- (d) clearly understand the respective responsibilities of each institution.
- (e) with respect to payable through accounts the financial institution should be satisfied that where customers of the respondent bank that have direct access to its accounts, the respondent bank has performed CDD obligations on its customers that have direct access to the accounts of the correspondent banks; and is able to provide relevant CDD information to the financial institution upon request.

20. Referred to the sub-section (d-2), section 28, Chapter (8) of the Anti-Money Laundering Law, regarding the information exchange, group-level compliance, audit, and AML/CFT functions should be provided with customer, account, and transaction information from bank branches and subsidiaries when necessary for AML/CFT purposes.

21. Financial institutions are required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements, where the minimum AML/CFT requirements of the host country



are less strict than those of the home country, to the extent that host country laws and regulations permit. If the host country does not permit the proper implementation of AML/CFT measures consistent with the home country requirements, financial groups should be required to apply appropriate additional measures to manage the ML/TF risks, and inform their home supervisors.

22. In dealing with countries that do not sufficiently comply with measures on money laundering and terrorist financing identified in the sub-section (a), section 31, chapter (8) of the Anti-Money Laundering Law, the following shall be conducted:

- (a) Reporting organizations shall apply enhanced CDD measures proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries, regions with inadequate AML/CFT systems and if it is necessary, shall apply countermeasures, proportionate to the risks, when called upon by international AML/CFT organizations including the Financial Action Task Force and the Asia Pacific Group on Money Laundering or other similar regional body.
- (b) The FIU may direct that reporting organizations impose enhanced CDD measures or counter-measures on to business relationships and transactions with natural and legal persons (including financial institutions), proportionate to the risks, 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.

23. When competent authorities assess the risk of ML and FT at the Reporting Organization in accordance with sub-section (b), section 36, chapter (8) of the Anti-Money Laundering Law, the assessment shall be conducted periodically or when there

are major events or developments in the management and operations of the Reporting Organization or group.

24. Competent authorities shall conduct on-site and off-site supervisory activities at such intervals as may be determined by the competent authority pursuant to a risk-based approach to supervision undertaken by them to determine whether reporting organizations have complied with their obligations.

25. Competent authorities, where not otherwise provided for in other laws, develop and implement appropriate financial and other fitness and proprietary requirements while registering, licensing or issuing permissions to reporting organizations and while approving those owning, to prevent criminals or their associates from owning or controlling, or participating, directly or indirectly, in the establishment, management or operation or business of such reporting organizations, including the beneficial owner or beneficiary of such shares of the institution.

26. The competent authority may take one or more of the following actions against reporting organizations, or the directors, board of directors, executive officers or managers of such organizations who fail to comply with the duties contained in Chapter VIII.

- (a) Give a warning in writing;
  - (b) Restrict with specific instructions;
  - (c) Compel submission of reports relating to the identified violation in accordance with the specifications;
  - (d) Take appropriate administrative actions that include suspending within a specific period, revoking, prohibiting, or suspending license or registration;
  - (e) a fine minimum 5 million to maximum 100 million to those who fail to comply with in this law;
27. (a) Any director, partner, officer principal or employee responsible person from a reporting organization and a customer shall not, except under the provision of



an existing law, disclose to anyone that any report or other information under section 38 are being sent or were sent to the Financial Intelligence Unit, that money laundering or terrorist financing investigations are being conducted, or have been conducted;

- (b) The provision in subsection (a) shall not apply to disclosures made as a duty, with respect to the implementation of anti-money laundering or countering of financing of terrorism measures under this Law, or any other existing law.

28. When the Customs Department provides information in accordance with section 42, Chapter (10) of the Anti-Money Laundering Law, the Customs Department shall ensure that this information is made available upon request to other relevant authorities including Financial Intelligent Unit, Central Bank of Myanmar, Immigration authorities, tax authorities, and law enforcement agencies.

29. Regarding international cooperation, as per Chapter (12) of the Anti-Money Laundering Law, if exchange of information with foreign counterparts is not available in other laws, the following shall be carried out:

- (a) Financial supervisors can exchange information which is available to them domestically with foreign counterparts for purposes related to the AML Law.
- (b) The information will be exchanged in a manner proportionate to the respective needs of their foreign counterparts.
- (c) Financial supervisors should be able to conduct inquiries on behalf of their foreign counterparts, and, as appropriate, to authorize or facilitate the ability of foreign counterparts to conduct inquiries themselves in the country, in order to facilitate effective group supervision.
- (d) Where financial supervisors have a shared responsibility for financial institutions operating in the same group, they can exchange the following types of information, as may be required.

- (1) regulatory information, such as information on the domestic regulatory system and general information on the financial sectors
  - (2) prudential information, such as information on the financial institution's business activities, beneficial ownership, management, and fit and properness, and
  - (3) AML/CFT information such as internal AML/CFT procedures and policies of financial institutions, customer due diligence information, customer files, samples of accounts and transaction information
- (e) The relevant law enforcement authorities can exchange information which is available to them domestically with foreign counterparts for intelligence and investigative purposes related to money laundering, its associated predicate offences and terrorist financing,
- (f) The relevant law enforcement authorities can use all powers available to them to exchange information,
- (g) The relevant competent authorities can exchange information, as may be relevant with non-counterparts, for purposes related to money laundering, its associated predicate offences and terrorist financing.

30. Lawyers, notaries and legal professionals and accountants engaging in a transaction for their customer or on their behalf, are required to submit to the Financial Intelligence Unit, the information upon which the suspicion is based and not given by or obtained from the customer, along with other relevant information requested by the Financial Intelligence Unit.

31. Lawyers, notaries, legal professionals and accountants, in performing the task of checking the legal status of their client, defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings, obtain



information requiring professional secrecy or special legal rights, such information shall not be required to be submitted in a suspicious transaction report.

32. For purposes relating to the money laundering offence described in Section (5), Chapter 3 of the Law and article 3 of this order, the prosecution body shall conduct its duties in accordance with section 61, chapter (15). In prosecutions, a conviction for the offence that has generated the proceeds or for property obtained by illegal means shall not be necessary to prove that the property is directly or indirectly the proceeds of crime or property obtained by illegal means.

33. Whoever fails to comply with the order shall, on conviction, be punished with a prison term in line with the provisions of the Anti-Money Laundering Law.