30 June 2019

AML/CFT Guidelines for Financial Institutions and Designated Non-Financial Businesses and Professions

1. PURPOSE

These Guidelines offer guidance to Financial Institutions and Designated Non-Financial Businesses and Professions on the provisions of the AML Laws in respect of Financial Institutions and DNFBPs.

The recommendations set out in these Guidelines are provided by DMCCA based on its own interpretation of the requirements of the AML Laws. As such these recommendations are not mandatory rules and regulations of the DMCC Free Zone. Rather, it is the responsibility of each Financial Institution or DNFBP to review its responsibilities under the AML Laws fully and carefully to determine the extent to which they implement the requirements of the AML Laws in respect of their own business and policies. These Guidelines are not intended to be, nor should they be construed as, legal advice.

2. RECOMMENDATION ONE – COMPLIANCE PROGRAMME

2.1. Financial Institutions and DNFBPs are advised to:

i) Establish, implement, monitor, and maintain an effective compliance program in line with these Guidelines.

ii) Devise and implement relevant policies, procedures, processes and controls designed to prevent and detect potential Money Laundering, Terrorist Financing activities.

iii) Appoint a compliance officer at management level or a designated focal point for compliance related matters who will be responsible for the day-to-day oversight of relevant policies, procedures, processes and controls to detect, prevent Money Laundering, Terrorist Financing.

iv) Ensure that relevant policies, procedures, processes and controls are communicated to all relevant employees.

v) Establish ongoing employees training program to ensure that they are kept informed of new regulations, developments, risks, techniques, methods and trends.

vi) Ensure an independent review system that will test and assess the effectiveness of these Guidelines on a risk-sensitive basis; this review shall have a defined minimum frequency.

vii) Devise and implement appropriate screening procedures to ensure that employees, customers and suppliers are not identified on any official sanctions list.

3. RECOMMENDATION TWO – DUTIES OF COMPLIANCE OFFICERS

3.1. It is recommended that the compliance officer be responsible for:

i) Investigating transactions related to alleged crimes.

ii) Reviewing and updating systems and internal procedures.

iii) Developing, implementing, monitoring, and maintaining appropriate ongoing training and awareness programmes.

iv) Producing biannual reports to senior management concerning adherence to compliance policies, procedures, processes and controls and sending a copy of them to the relevant Supervisory Authority with senior managements' comments and decisions.

v) Receiving internal suspicious transaction/activity reporting submitted by their employees, investigating the internal suspicious activity and taking appropriate action including, where appropriate, making external Suspicious Transaction Reports (**"STR"**) to the Financial Intelligence Unit of (**"FIU"**) and send a copy to DMCCA.

vi) Acting as the point of contact to the DMCCA and relevant agencies concerned with AML/CFT matters, and responding promptly to any request for information made by any Competent Authority and/or Supervisory Authority.

vii) Notifying DMCCA promptly regarding any communication from other authorities concerning Money Laundering and Terrorist Financing matters.

4. RECOMMENDATION THREE – DUE DILIGENCE

4.1. Financial Institutions and DNFBPs are advised to:

i) Properly identify its customers, and maintain customer identification records including reliable documentation. Such customer identification records will require to be made available to DMCCA or to any other Competent Authority promptly upon request.

ii) Adopt a risk based approach to determine the extent of additional due diligence measures with the level of risk posed by the customer type, business relationship, transaction, product/service or geographical location.

iii) Conduct enhanced due diligence measures when there is a suspicion of Money Laundering, Terrorist Financing activity, or where high risk circumstances are identified.

iv) Have an independent audit position to assess the efficiency and adequacy of the policies, controls and procedures.

v) undertake due diligence measures in the following cases:

- establishing the business relationship;
- carrying out occasional transactions in favour of a customer for amounts equal to or exceeding AED 55,000, whether the transaction is carried out in a single transaction or in several transactions that appear to be linked;
- carrying out occasional transactions in the form of wire transfers for amounts equal to or exceeding AED 3,500;
- where there is a suspicion of Money Laundering, Terrorist Financing;
- where there are doubts about the veracity or adequacy of previously obtained customer's identification data;
- on an annual basis;
- at periodic intervals based on company status and circumstances.

4.2 Due diligence measures comprise the following:

i) identifying the customer and, where applicable, the customer's ultimate beneficial owner to 25% or more of controlling share by natural person, any person acting on behalf of a customer or senior management officer if cannot identify natural person.

ii) verifying the customer's identity on the basis of reliable and independent information, data or documentation to at least the extent required by the applicable legal and regulatory framework.

4.3 The following documentation in respect to natural persons and legal entities should be requested.

a) for verification of the identity of a natural person:

i) applicant's full name (as per NID or passport);
ii) date and place of birth;
iii) nationality;
iv) physical address (residential and business / home country and UAE);
v) contact details;

b) for verification of the identity of a legal entity:

i) full business name, including any trading name;
ii) registered or business address with contact details;
iii) place of incorporation or registration;
iv) valid commercial or professional license;

v) the identity of the directors, managers, shareholders, signatories or equivalent persons with executive authority in respect of the legal entity;
vi) ultimate beneficial owners;
vii) copy of memorandum and articles of association.

4.4 Financial Institutions and DNFBPs are advised to understand the purpose and intended nature of the business relationship and, obtain further information to conduct sustained follow-up; including but not limited to the following:

i) confirming authority to act on behalf of a customer;
ii) previous business activities / experience;
iii) purpose of intended relationship;
iv) anticipated type and volume of activities; and
v) auditing transactions of customers for consistency (know their business).

5. RECOMMENDATION FOUR – RISK ASSESSMENT

Financial Institutions and DNFBPs are advised to:

a. Identify AML/CFT risks within the business's scope of work as well as continuously assess, document, and update such assessment based on the various risk factors established in the relevant legislation.
b. Refrain from opening or conducting any financial or commercial transaction under an anonymous or fictitious name or by pseudonym or number, and maintaining a relationship or providing any services to it.
c. Maintain AML/CFT prevention policies, procedures, processes and controls that are relevant and up-to-date in line with the dynamic risk associated with its business, products and services and that of its customers.
d. Establish, implement, monitor, and maintain satisfactory controls that are in line with the level of AML/CFT prevention risk.

6. RECOMMENDATION FIVE –RELIANCE ON THIRD PARTIES

6.1. Financial Institutions and DNFBPs may outsource the technical aspects of any compliance process to qualified service providers duly regulated and supervised in the country where they are based and incorporated, provided that:
6.1.1. Service provider information is obtained in accordance with the due diligence measures referred to in Recommendation Three,

6.1.2. Identification data and other relevant documentation relating to due diligence is available promptly upon request.

6.2. The ultimate responsibility for customer identification and verification, and any other outsourced function, is that of the Financial Institution or DNFBP regardless of the arrangements entered with any service provider.

6.3. There are no secrecy or data protection issues that would restrict prompt access to data, or impede the full application of the AML Laws with respect to any outsourced relationship.

7. RECOMMENDATION SIX – INTERNAL AND EXTERNAL REPORTING

7.1. Financial Institutions and DNFBPs are advised to have relevant policies, procedures, processes and controls in place for the purposes of detecting Money Laundering, Terrorist Financing that enable employees to report to the compliance officer any suspicion or knowledge of Money Laundering, Terrorist Financing activity that is identified.

7.2. If a DNFBP suspects or has reasonable grounds to suspect that funds concerning an actual or proposed transaction are the proceeds of any criminal activity, or are related to Money Laundering, Terrorist Financing activity, the compliance officer is advised to promptly file a written STR with the FIU.

7.3. The compliance officer is advised to make every employee aware of his/her role and duty to receive or submit internal suspicious activity reports.

7.4. The compliance officer is advised to investigate STRs internally and create an internal report outlining the outcome of its investigation including the decision on whether or not to file an external STR. Where appropriate, the compliance officer is advised to make the STR to the FIU and provide a copy to DMCCA.

7.5. Where applicable, the background and purpose of the activity in question may be examined by the compliance officer and findings may be established in writing.

7.6. In the event the compliance officer concludes that no external report should be made, the justification of such a decision should be recorded.

8. RECOMMENDATION SEVEN– NON-DISCLOSURE OF REPORTING

8.1. Confidentiality is key to maintain the integrity of an investigation in respect of any Suspicious Transaction/Activity. A person reporting a Suspicious Transaction/Activity or making a STR is prohibited from disclosing to the subject of the reporting or any third party that:

(i) a Suspicious Transaction/Activity has been reported;
(ii) enquiries are being made; or

(iii) criminal investigations are being carried out as a result of an STR.

9. RECOMMENDATION EIGHT – REGULATORY COOPERATION

Where a Financial Institution or DNFBP receives a request for information or inspection from any Competent Authority and/or Supervisory Authority regarding enquiries into potential Money Laundering, Terrorist Financing activity carried on, they should respond promptly. Financial Institutions and DNFBPs shall maintain a risk identification and assessment analysis with supporting data to be provided to the Supervisory Authority upon request.

10. RECOMMENDATION NINE– STAFF AWARENESS AND TRAINING

10.1. It is advised to establish on-going and up-to-date relevant AML/CFT prevention employee training that appropriately covers responsibilities under the AML Laws and corresponding regulations, policies, procedures, processes and controls.

10.2. Employees shall be kept informed of up-to-date risk vulnerabilities, including information on current AML/CFT prevention techniques, methods and trends.

10.3. Training shall be sufficiently tailored in its content and frequency to the operations and the type of business and the context of the employees function.

10.4. Except in respect of senior managers and compliance officer whose training must be provided immediately on assumption of their duties, a Financial Institution or DNFBP is advised to ensure that all relevant employees receive appropriate training within 60 days of commencement of employment.

11. RECOMMENDATION TEN– RECORD KEEPING

11.1. Financial Institutions and DNFBPs are advised to maintain all records, documents, files and data in respect of all local or international financial transactions in a well-organized manner, for at least five years (5) years starting from the date of completion of a transaction or of the end of the business relationship with a customer.

11.2. All records and documents obtained through the due diligence measures, and the accounting files, commercial correspondence, copies of the personal identification documents, including suspicious transactions reports and the results of any analysis that was conducted, shall be kept for at least five years (5) years starting from the date of the end of a business relationship. Responsibilities for storage, retention, processing, protection and destruction of such records should form part of the company's data protection and retention policies.

11.3. Financial Institutions and DNFBPs are advised to maintain records including dates of training sessions, a description of training provided and names of the employees that received training for a period of at least five (5) years from the date on which training was received.

11.4. The transaction records and other identification data may be made available to the any Competent Authority and/or Supervisory Authority upon request.

12. DEFINITIONS

Unless otherwise stated, a capitalised term used in these Guidelines has the following meanings (failing which has the meaning given to that term in the AML Laws):

AML Laws	The Decree-Law and the Executive Regulation, taken together.
Competent Authorities	The competent government authorities in the State entrusted with the implementation of any provision of this Decree law.
Decree-Law	Federal Decree- Law No. (20) of 2018 on Anti-Money Laundering and Combatting the Financing of Terrorism and Financing of Illegal Organizations
Designated Non-Financial Business and Professions or DNFBPs	• Real estate brokers and agents; • Precious metals and stones traders when carrying any single monetary operation or several apparently interrelated operations whose value is equal to or more than AED 55,000; • Lawyers, notaries and accountants; and • Corporate service and/or trust fund providers. • Other businesses/professions specified by Ministry Decision
DMCC	the Dubai Multi Commodities Centre

DMCCA	the Dubai Multi Commodities Centre Authority, established pursuant to Law No. 4 of 2001 and by virtue of Decision No. 4 of 2002, each issued in the Emirate of Dubai, which authority has governance over the DMCC Free Zone as a Competent Authority for the purposes of Decree- Law.
Executive Regulation	Cabinet Decision No. (10) of 2019 on the Executive Regulation of Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering and Combatting the Financing of Terrorism and Financing of Illegal Organizations
Supervisory Authority	Federal and local authorities which are entrusted by legislation to supervise Financial Institutions, Designated Non-Financial Businesses and Professions and Non-Profit Organisations or the Competent Authority in charge of approving the pursuit of an activity or a profession in case a supervisory authority is not assigned by legislations.
Suspicious Transaction Report (STR)	A report made by a DNFBP to the FIU about suspicious or potentially suspicious activity, related to the money laundering, financing of terrorism or of illegal organisations.
Financial Intelligence Unit (FIU)	Financial Intelligence Unit of the Central Bank of the UAE.