GUIDANCE FOR RISK-BASED COMPLIANCE FOR Designated Non-Financials Business and Professions - DNFBPs: G - 01

GLOSSARY OF TERMS USED IN THE GUIDANCE

Defined Term	Definition
AML/CFT	Anti Money Laundering and Combating the Financing of Terrorism
AMLSCU	The Anti Money Laundering Suspicious Cases Unit of the UAE;
CDD	Customer Due Diligence
DMCCA	**Dubai Multi Commodities Centre Authority**
Competent Authority	All administrative and law enforcement authorities concerned with combating Money Laundering, Terrorist Financing and Fraud activity, including the AMLSCU supervisors and DMCCA
EDD	Enhanced Due Diligence
Money Laundering	A criminal offence defined in article (1) of the Federal law No 4 of 2002 of the UAE.
DNFBP	Designated Non-Financial Businesses and Professions.
Terrorism Financing	as defined by UN Resolution 54/109 issued by the United Nations 1999 International Convention for the Suppression of the Financing of Terrorism
SAR	Suspicious Activity Report
UAE	United Arab Emirates

1. INTRODUCTION

1.1. PURPOSE

These Guidelines have been compiled to offer guidance to Designated Non-Financial Businesses and Professions ("DNFBP's") on how best to comply with Anti-Money Laundering ("AML"), Combating Financing of Terrorism ("CFT") and Fraud Prevention ("FP) legislation and Best Practices applicable to their business.

The recommendations set out in these Guidelines are not mandatory and it is up to each DNFBP to determine the extent to which they implement such recommendations.

Each DNFBP is responsible for his own policies and implementation and should not rely on this publication other than as a general framework and guideline.

1.2. POTENTIAL BENEFITS

In following these Guidelines, DNFBP's may benefit from an increased awareness and understanding of AML, CFT and FP legislation and Best Practices applicable to their business thereby

i) Reducing the risk of their breaching any AML, CFT and FP provisions, and

ii) Reducing any potential reputational or financial loss.

1.3. DISCLAIMER

These Guidelines are not intended to be, nor should they be construed as, legal advice. Legislation, regulations and directives etc are all subject to amendment, cancellation and variation by their issuing authorities and these Guidelines may not be an accurate representation of such existing legislation at the time of their publication.

As such, and for a definitive opinion as to AML, CFT and FP matters, DNFBP's are advised to seek independent legal advice from reputable law firms where deemed appropriate.

2. GENERAL APPLICATION

2.1. These Guidelines are intended to offer guidance for all DNFBP's registered as DMCC / JLT members, typically they include:

2.1.1. Real estate agents involved in transactions for or on behalf of a client concerning the buying, leasing or selling of real estate in relation to both the purchasers and vendors of property.

2.1.2. Wholesale dealers or manufacturers in precious metals and precious stones

2.1.3. Lawyers, notaries, other independent legal professionals and accountants, including auditing service providers who prepare or carry out transactions for their clients, including but not limited to:

2.1.3.1. Buying , leasing or selling of real estate;

2.1.3.2. Managing of client money, securities or other assets;

2.1.3.3. Management of bank, savings or securities accounts other than as a business that meets the definition of financial institution;

2.1.3.4. Organisation of contributions for the creation, operation or management of companies;

2.1.3.5. Creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

2.1.4. Company service providers, when they prepare for or carry out transactions for a client including but not limited to:

2.1.4.1. Acting as a formation agent of a legal person or entity;

2.1.4.2. Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or like positions in relation to other persons or legal structures;

2.1.4.3. Providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; or

2.1.4.4. Acting as (or facilitating for any third party) a nominee shareholder.

3. RECOMMENDATION ONE – COMPLIANCE REQUIREMENTS

A DNFBP is advised to:

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

3.2. Devise and implement relevant policies, procedures, processes and controls designed to prevent and detect potential Money Laundering, Terrorist Financing and Fraud activities. Such measures should consider the following:

3.2.1. Compliance Regime;

3.2.2. Risk Assessment;

3.2.3. Customer Due Diligence;

3.2.4. Record retention;

3.2.5. Training and awareness;

3.2.6. Employee screening;

3.2.7. Detection of unusual and/or suspicious transactions; and

3.2.8. Monitoring and Reporting

3.3. Appoint a compliance officer at a 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 and Fraud.

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

3.5. Establish ongoing employees training program to ensure that they are kept informed of new developments, including information on current anti Money Laundering, anti Terrorist Financing and anti Fraud risks, techniques, methods and trends.

3.6. 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.

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

4. RECOMMENDATION TWO – COMPLIANCE PROGRAMME

4.1. It is advisable for a DNFBP's Senior Management to ensure that a compliance programme in line with these guidelines is executed and managed appropriately.

4.2. A DNFBP is advised to appoint a Compliance Officer or a designated focal point for compliance related matters responsible for establishing and maintaining policies, procedures, processes and controls consistent with UAE AML/CFT legislation and guidelines applicable in DMCC, and exercising day-to-day operational oversight of the DNFBP's compliance functions.

4.3. It is recommended that the Compliance Officer's responsibilities also include identifying and undertaking appropriate action on matters of Money Laundering, Terrorist Financing or Fraud concerns that are identified as part of the risk assessment process or by queries of various authorities.

4.4. It is recommended that the Compliance Officer be responsible for:

4.4.1. Establishing, implementing, monitoring, and maintaining an appropriate ongoing programme of AML / CFT and Fraud prevention training and awareness, and

4.4.2. Producing annual reports to senior management concerning the level of compliance adherence to policies, procedures, processes and controls.

4.5. It is recommended that the Compliance Officer be responsible for receiving internal suspicious activity reports submitted by employees of the DNFBP, investigating the internal suspicious activity report and taking appropriate action which would include, where appropriate, making external suspicious activity reports to the AMLCSU and send a copy to DMCCA.

4.6. The Compliance Officer would also be responsible for acting as the point of contact to the DMCCA and relevant agencies concerned with AML/CFT and Fraud matters, and responding promptly to any request for information made by DMCCA or other Competent Authorities of the UAE.

4.7. The Compliance Officer would notify DMCCA promptly regarding any communication from other authorities or regulators concerning Money Laundering, Terrorist Financing or Fraud matters.

4.8. A DNFBP is advised to make appropriate provisions for any absence of the Compliance Officer and appoint a suitable deputy to assume the responsibilities set out above.

4.9. It is recommended that the Compliance Officer have the requisite experience and independence to act on his/her own authority, have direct access to senior management, and have sufficient resources including appropriately trained and effective staff.

4.10. It is recommended that the Compliance Officer has access to relevant information concerning the DNFBP's clients, representatives of the clients, business relationships and transactions and the details of such transactions which a DNFBP contemplates or actually enters into, with or for a client or third-party.

4.11. A DNFBP is advised to commission an annual report from its Compliance Officer, that will report the level of compliance adherence to relevant policies, procedures, processes and controls with respect to regulatory obligations.

4.12. The DMCCA will issue relevant guidance and conduct necessary training for the proper implementation of Recommendation 2.

5. RECOMMENDATION THREE – CLIENT DUE DILIGENCE (CDD)

5.1. GENERAL

A DNFBP is advised to:

5.1.1. Properly identify its clients, and maintain client identification records including reliable documentation. Such client identification records will require to be made available to DMCCA or to any Competent Authority promptly upon request.

5.1.2. Adopt a risk based approach to determine the extent of additional CDD measures commensurate with the level of risk posed by the client type, business relationship, transaction, product/service or geographical location.

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

5.2. TIMING

A DNFBP is advised to:

5.2.1. Undertake satisfactory CDD measures when:

5.2.1.1. Establishing a business relationship;

5.2.1.2. There is any suspicion of Money Laundering , Terrorist Financing or Fraud; or

5.2.1.3. The DNFBP has doubts about the integrity or adequacy of previously obtained client identification data

5.2.1.4. Updating the CDD information on an annual basis

5.2.2. Verify the identity of each client and beneficial owner when establishing a

business relationship or conducting transactions for irregular clients.

5.3. APPLICATION

5.3.1. A DNFBP is advised to implement the following standards of CDD measures:

5.3.1.1. Identify and verify the identity of a Client that is a natural person, using relevant and reliable independent source documents, data or information (Identification Data);

5.3.1.2. If the client is not a natural person the DNFBP may:

5.3.1.2.1. Identify and verify the name, address and legal status of the client by obtaining proof of incorporation issued by the relevant authority, or similar formal evidence of establishment and existence;

5.3.1.2.2. Verify that any person purporting to act on behalf of the client is authorized to do so, and that such person's identity is properly verified; and

5.3.1.2.3. Identify the beneficial owner, taking reasonable measures to verify the identity of the beneficial owner using identification data obtained such that the DNFBP is satisfied that it recognizes who the beneficial owner(s) are; and

5.3.1.2.4. Understand the ownership and control structure of the client; and

5.3.1.2.5. Identify the natural persons that may ultimately own and control the client.

5.3.1.3. Establish and record the purpose and intended nature of the business relationship; and

5.3.1.4. Conduct ongoing due diligence on the business relationship and apply scrutiny to transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the DNFBP's knowledge of the particular clients, their business and risk profile, including, where necessary, the source of funds.

5.3.2. A DNFBP is advised to ensure that identification data is kept up-to-date and may review the records of higher risk customers or business relationships as appropriate.

5.3.3. Where a DNFBP is unable to comply with any of the CDD measures, it is advised not to open an account, commence business relations, accept instructions or perform the transaction.

5.3.4. Where CDD obligations for existing business relationships and clients are not met, as a result of the client's refusal to comply or causing unacceptable delays, the DNFBP is advised to terminate the business relationship, and consider making a Suspicious Activity Report (SAR) to the AMLSCU, sending relative copies to the DMCCA.

5.3.5. It is recommended that these CDD measures apply to all of DNFBP's new clients. A DNFBP is advised to apply relevant CDD measures to existing clients in situation where:

5.3.5.1. The client's documentation standards are changed substantially with the introduction of compliance requirements with these guidelines; or

5.3.5.2. There is a material change in the nature of the relationship with the client; or

5.3.5.3. The DNFBP becomes aware that it lacks sufficient information about an existing client, or is concerned of the accuracy of information recorded

6. RECOMMENDATION FOUR – RISK ASSESSMENT

A DNFBP is advised to:

6.1. Adequately assess its AML/CFT and Fraud risks in relation to its clients, its business, products and services, geographical exposures and appropriately define and document its risk-based approach.

6.2. Maintain AML/CFT and fraud 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 clients.

6.3. Establish, implement, monitor, and maintain satisfactory controls that are commensurate with the level of AML/CFT and fraud prevention risk.

6.4. The DMCCA will issue relevant guidance and conduct necessary training for the proper implementation of Recommendation 4.

7. RECOMMENDATION FIVE – ENHANCED DUE DILIGENCE (EDD)

A DNFBP is advised to:

7.1. Perform enhanced due diligence (EDD) for higher risk categories of customers, business relationships or transaction.

7.2. Ensure it is aware of new or developing technologies that might favour anonymity and take measures to prevent their use for the purpose of Money Laundering, Terrorist Financing or Fraud.

7.3. Apply enhanced due diligence in the following circumstances:

7.3.1. HIGH RISK PARTIES

7.3.1.1. In assessing the risks in relation to Money Laundering , Terrorist Financing or Fraud , a DNFBP is advised to give special attention to business relationships established and transactions intended or conducted with persons and entities from or in countries that do not apply, or insufficiently apply, AML/CFT and Fraud Prevention rules, as identified by:

7.3.1.1.1. The Government of the UAE or any government

7.3.1.1.2. The Central Bank of the UAE or the AMLSCU;

7.3.1.1.3. The DMCCA

7.3.1.1.4. The Gulf Cooperation Council;

7.3.1.1.5. The Financial Actions Task Force (FATF);

7.3.1.1.6. Middle East & North Africa Financial Action Task Force

7.3.1.2. A DNFBP is advised to apply systems and controls that can appropriately identify and manage the enhanced risk associated with clients or transactions in or from countries that are prone to corruption, terrorism or conflicts.

7.3.1.3. A DNFBP is advised to make appropriate use of relevant findings issued by any of the above authorities concerning any named individuals, groups or entities that are the subject of money laundering, terrorist financing or fraud concerns or included in sanctions lists issued by international competent authorities. Regarding various individuals and entities, it is recommended that DNFBP should know prior to establishing a customer relationship;

A.) Who is this person?

B.) What type of activity does he/she want to conduct with my

company? C.) What type of pattern of activity can I expect?

D.) Is he/she representing a third party?

E.) How can I verify the information presented to me?

7.3.2. NON FACE-TO-FACE BUSINESS

7.3.2.1. When conducting non-face-to-face business with clients that have not been physically present for the purposes of identification and verification, the DNFBP is advised to have policies, procedures, systems and controls in place to manage specific risks associated with such non-face to face business, relationships or transactions.

7.3.2.2. A DNFBP is advised to, at a minimum; require one piece of formal identification which have been certified appropriately and one formal document that will verify the physical address of the client. Where the client is a legal person, a DNFBP is recommended to require documentary evidence of the continuing existence of the legal person (good standing certificate) and a certified copy of acceptable identification and address documentation to verify the address of any person defined 5.3.1

7.3.2.3. A DNFBP is advised to ensure that adequate procedures for monitoring activity of non-face to face business are implemented and managed

effectively.

7.3.2.4. The DMCCA will issue relevant guidance and conduct necessary training for the implementation of Recommendation Five.

8. RECOMMENDATION SIX – OUTSOURCING

8.1. A DNFBP may outsource the technical aspects of Compliance process only to qualified service providers duly regulated and supervised in the country where they are based and incorporated, as long as such outsourcing allows for:

8.1.1. The DNFBP to promptly obtain from the Compliance Service Provider the information under Recommendation Three; and

8.1.2. The DNFBP's ability to obtain copies of Identification Data and other relevant documentation relating to CDD requirements promptly upon request.

8.2. The ultimate responsibility for client identification and verification, and any other outsourced function, is that of the DNFBP regardless of the arrangements entered with any Compliance Service Provider.

8.3. A DNFBP is advised to ensure that there are no secrecy or data protection issues that would restrict prompt access to data, or impede the full application of these Guidelines with respect to any outsourced relationship.

8.4. The DMCCA will issue relevant guidance and conduct necessary training for the implementation of Recommendation Six.

9. RECOMMENDATION SEVEN – SUSPICIOUS ACTIVITY AND MONITORING

9.1. A DNFBP is advised to routinely monitor for and detect suspicious activity, and is recommended to, at a minimum, examine the background and purpose of the following:

9.2. Complex or unusually large transactions, which have no apparent visible economic or lawful purpose.

9.3. Transactions outside the usual pattern of the client's activity as known to the DNFBP.

9.4. Transactions that are deemed to be of high risk with regard to a client or business relationship, or as they relate to high risk geography, products or services.

9.5. Transactions, clients, or business relationships that cause the DNFBP to have reasonable grounds to suspect money laundering, terrorist financing or Fraud.

9.6. The DMCCA will issue relevant guidance and conduct necessary training for the implementation of Recommendation Seven.

10. RECOMMENDATION EIGHT – INTERNAL AND EXTERNAL REPORTING

10.1. A DNFBP is advised to have relevant policies, procedures, processes and controls in place for the purposes of detecting Money Laundering, Terrorist Financing or Fraud that enable an employee to report to the Compliance Officer any suspicion or knowledge of Money Laundering, Terrorist Financing or Fraud activity that is identified.

10.2. 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 or Fraud activity, the Compliance Officer is advised to promptly file a written SAR with the AMLSCU and provide a copy to DMCCA.

10.3. The Compliance Officer is advised to make every employee aware of his/her role and duty to receive or submit internal suspicious activity reports.

10.4. The Compliance Officer is advised to investigate SAR's internally, build an internal report outlining the outcome of his investigation including the decision on whether or not to file an external SAR. Where appropriate the Compliance Officer is advised to make the SAR to the AMLSCU and provide a copy to DMCCA.

10.5. Where applicable, the background and purpose of the activity in question may be examined by the Compliance Officer and the findings may be established in writing.

10.6. In the event the Compliance Officer concludes that no external report should be made, the justification of such a decision may be recorded.

10.7. A DNFBP is advised to institute disciplinary measures against any employee that fails to make an internal suspicious activity report where there are grounds for him/her to do so.

10.8. The DMCCA will issue relevant guidance and conduct necessary training for the implementation of Recommendation 8.

11. RECOMMENDATION NINE – NON-DISCLOSURE OF REPORTING

11.1. DNFBPs, their directors, officers and employees (permanent and temporary) are advised not to disclose to the subject or any person other than one with a legitimate right or need to know, the fact that a SAR or related information has been or will be reported or provided to the Compliance Officer, the AMLSCU or the DMCCA.

12. RECOMMENDATION TEN – REGULATORY COOPERATION

12.1. Where a DNFBP receives a request for information from any Competent Authority regarding enquiries into potential Money Laundering, Terrorist Financing or Fraud activity carried on, the DNFBP is advised to promptly inform the DMCCA in writing.

12.2. A DNFBP is advised to respond promptly to any appropriate request for information or inspection that is issued by the DMCCA.

13. RECOMMENDATION ELEVEN – STAFF AWARENESS AND TRAINING

13.1. A DNFBP is advised to establish on-going and up-to-date relevant AML/CFT and Fraud Prevention employee training that appropriately covers their obligations under the laws, regulations, policy procedures, processes and controls.

13.2. A DNFBP is advised to establish measures to ensure that employees are kept informed of up-to-date risk vulnerabilities, including information on current AML/CFT and Fraud prevention techniques, methods and trends.

13.3. A DNFBP is advised to ensure that training is sufficiently tailored in its content and frequency to the operations and business of the DNFBP, its employees, and its clients.

13.4. A DNFBP is advised to keep employees informed on an ongoing basis of the type of suspicious activity that is pertinent to the type of business of the DNFBP and to the context of the employees function.

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

13.6. The DMCCA will issue relevant guidance and conduct necessary training for the implementation of Recommendation Eleven.

14. RECOMMENDATION TWELVE – RECORD KEEPING

14.1. A DNFBP is advised to maintain all records on the KYC documentation and on any transaction for at least five years (5) years following the establishment of the relationship or the completion of the transaction, regardless of whether the account or business relationship is ongoing or has been terminated.

14.2. Where maintenance of client records is outsourced to qualified service providers in accordance with Recommendation Seven, DNFBPs are advised to take reasonable steps to ensure that such records are held in a manner that conforms to these Guidelines.

14.3. A DNFBP is advised to maintain information, correspondence and documentation for client identification and verification, and associated due diligence for a period of at least five (5) years from the end of the business relationship with the client or the last transaction conducted.

14.4. A DNFBP is advised to maintain records in accordance with Recommendation Eight concerning the internal reporting of unusual or suspicious transactions and all records of investigations of those reports together with the decision made may be retained for at least a period of five (5) years after the report has been made.

14.5. A DNFBP is 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.

14.6. A DNFBP is advised to maintain records of the annual report, and any other reports that highlight the level of compliance, deficiencies and actions, including reports submitted to senior management.

14.7. The transaction records and other identification data may be made available to the DMCCA, or any other Competent Authority upon request.