Nasdaq Dubai

Nasdaq Dubai Notice No. : 73/2019
Date of Issue : 22 October 2019
Date of Expiry : Once published in Nasdaq Dubai Business Rules

---

ANTI- MONEY LAUNDERING NOTICE
Rule 2.19

1. Introduction

1.1 This is the Anti-Money Laundering Notice referred to at Rule 2.19. It sets out the Anti-Money laundering regime which Nasdaq Dubai requires its Members to comply with and each Member must comply with the provisions of this Notice and any Circular issued under this Notice.

1.2 Capitalised terms used in this Notice and not otherwise defined herein shall have the meaning set out in the Rules.

1.3 This Nasdaq Dubai Notice will be available on the website at www.nasdaqdubai.com

2. Background

Members are subject to and must comply with the following:

(i) UAE Federal Decree-law No.20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations;

(ii) UAE Federal Law No. 7 of 2014 on Combating Terrorism Offences

(iii) Cabinet Decision No. 10 of 2019 concerning the implementing regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations;

(iv) Article 20 of Cabinet Decision No. 20 of 2019 regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing and Proliferation of Weapons of Mass Destruction, and Related Resolutions.

(v) The UAE Penal Code;

(vi) Any other laws applicable in the UAE and/or DIFC in relation to Anti-Money Laundering compliance; and

(vii) International standards concerning Anti-Money Laundering, such as the International Organisation of Securities Commissions ("IOSCO") principles and the Financial Action Task Force ("FATF") Principles.

Guidance:

It is important to note that Money Laundering is a crime under UAE Federal Decree-law No.20*,* UAE Federal Law No. 7 *and* Cabinet Decision No. 10 *and is punishable against institutions and individuals by both fines and imprisonment.*

Money laundering is generally described as any transfer or deposit of illegally obtained money, or any transaction aimed at hiding or disguising the true, nature, origin, location and/or ownership of the proceeds of their criminal activities, so that it appears to have originated from a legitimate source, when in fact it has not and thereby avoid prosecution, conviction and confiscation of criminal funds. This includes the closely related subject of terrorist financing and international efforts to locate and cut off the funding of terrorists and their organisations. A Member must have Anti-Money Laundering policies, procedures, systems and controls which must include provisions designed to prevent money laundering and terrorist financing. Unless otherwise expressly provided, references to Anti Money Laundering, its policies, procedures, systems, controls and/or the regime shall automatically be taken to include the prevention of terrorist financing.

2.1 Authorised Firms

2.1.1 A Member that is an Authorised Firm must comply with the Anti- Money Laundering, Counter-Terrorist Financing and Sanctions module of the DFSA Rulebook ("AML Module").

2.1.2 Nasdaq Dubai requires the Member to appoint a Money Laundering Reporting Officer ("MLRO") who shall act as point of contact within the Member for all money laundering issues.

2.1.3 Where a Member has appointed a MLRO for the purposes of the AML Module, the same MLRO and the same deputy shall act as the MLRO and deputy respectively.

2.2 Recognised Members

Guidance:

*A Recognised Member is not subject to the DFSA AML Module, but will instead be subject to an Anti-Money Laundering regime in their own jurisdiction of incorporation or organisation and if different, in the jurisdiction from which they are operating as a Recognised Member (separately and collectively the "**RM AML Regime**")*

2.2.1 A Member that is a Recognised Member must comply with each RM AML Regime that is applicable to it.

2.2.2 In addition to Rule 2.2.1, a Recognised Member must:

1) implement, operate and monitor a detailed customer identification and verification process, which enables the Member to:

(i) verify the identity of the Customer and any Beneficial Owner on the basis of original or properly certified documents, data or information issued by or obtained from a reliable and independent source;

(ii) determine whether there are any Politically Exposed Persons ("PEPs") who are Beneficial Owners;

(iii) understand the Customer's source of funds and wealth;

(iv) undertake a risk-based assessment of every Customer's money laundering risk;

(v) assign the Customer a risk rating proportionate to the Customer's money laundering risks; and

(vi) undertake appropriate on-going due diligence of the Customer's business relationship.

2) establish and maintain policies, procedures, systems and controls in order to monitor and detect suspicious activity or transactions in relation to potential money laundering or terrorist financing. Policies, procedures, systems and controls must ensure that whenever any employee, acting in the ordinary course of his employment, either:

(i) knows;

(ii) suspects; or

(iii) has reasonable grounds for knowing or suspecting;

that a person is engaged in or attempting money laundering or terrorist financing, that employee promptly notifies their MLRO and provides the MLRO with all relevant details.

3) ensure that all relevant information, correspondence and documentation used to identify and verify a Customer's identity is retained for at least six (6) years from the date on which the business relationship with the Customer ended, or if that date is unclear, it shall be taken to have ended on the date of completion of the last Transaction;

4) make appropriate use of government, regulatory and international findings, resolutions and sanctions lists while carrying out Customer due diligence; and

5) provide appropriate training to all relevant employees at suitable and regular intervals. The training sessions should:

(i) be tailored to the employee's specific responsibilities;

(ii) have documented programmes, training and testing material; and

(iii) record the dates of training sessions and attendance records.

Guidance:

An individual's identity comprises their name and all other names used, permanent residential address, date and place of birth and nationality. For legal entities, identity means the company or business name, including any trading names, the registered office and any principal place of business.

Member's money laundering risk assessment policies and procedures, should inter alia address in respect of the Customer:

(i) the nature of the Customer, ownership and control (if any);

(ii) whether the Customer is politically exposed;

(iii) country of origin, residence, nationality, place of incorporation (if any);

(iv) the type of product or service; and

(v) the size and frequency of the Transaction(s);

It is possible that existing Customers may become deliberately or unintentionally involved in money laundering. It is therefore vital that all Members are vigilant and that all abnormal activity is identified and discretely researched, with particular reference to:

(i) monitoring activity during the course of its customer relationship to ensure that the activity is consistent with the Member's knowledge of the Customer, their business and risk rating;

(ii) paying particular attention to any complex or unusually large Transactions or unusual patterns of Transactions that have no apparent or visible economic or legitimate purpose;

(iii) enquiring into the background and purpose of the Transactions in (ii);

(iv) periodically reviewing the adequacy of the Customer due diligence information it holds on Customers and Beneficial Owners to ensure that the information is kept up to date, particularly for Customers with a high risk rating; and

(v) periodically reviewing each Customer to ensure that the risk rating assigned to a Customer remains appropriate for the Customer in light of the money laundering risks.

Circumstances that might give rise to suspicion or reasonable grounds for suspicion include:

(i) Transactions which have no apparent purpose; which make no obvious economic sense; or which are designed or structured to avoid detection;

(ii) Transactions requested by a person without reasonable explanation, which are out of the ordinary range of services normally requested or are outside the experience of a relevant Person in relation to a particular customer;

(iii) where the size or pattern of transactions, without reasonable explanation, is out of line with any pattern that has previously emerged or are deliberately structured to avoid detection;

(iv) a customer's refusal to provide the information requested without reasonable explanation;

(v) where a customer who has just entered into a business relationship uses the relationship for a single transaction or for only a very short period of time;

(vi) an extensive use of offshore accounts, companies or structures in circumstances where the customer's economic needs do not support such requirements;

(vii) unnecessary routing of funds through third party accounts; or unusual transactions without an apparently profitable motive.

AML training should enable Member employees to:

(i) understand its policies, procedures, systems and controls relating to money laundering and any changes to these;

(ii) recognise and deal with transactions and other activities which may be related to money laundering;

(iii) understand the types of activity that may constitute suspicious activity in the context of the business in which an Employee is engaged and that may warrant a notification to the MLRO;

(iv) understand its arrangements regarding the making of a notification to the MLRO;

(v) be aware of the prevailing techniques, methods and trends in money laundering relevant to the business of the Member; and

(vi) understand the roles and responsibilities of employees in combating money laundering, including the identity and responsibility of the Member's MLRO and deputy, where applicable.

2.2.3 Nasdaq Dubai requires the Member to appoint a MLRO who shall act as point of contact within the Member for all money laundering issues.

2.2.4 The MLRO shall be responsible for all of the Member's anti money laundering activities carried on in or from the DIFC, and on or in connection with Nasdaq Dubai.

2.2.5 The MLRO must be acceptable to Nasdaq Dubai. The MLRO must be of sufficient seniority to act on his own authority, have direct access to the governing body and senior management of the Member, have sufficient resources to assist in the performance of his duties, have unrestricted access to the type of information about Customers and Transactions which Nasdaq Dubai would expect the MLRO to have access to.

2.2.6 the MLRO carries out and is responsible for:

1) establishing and maintaining the Member's anti-money laundering policies, procedures, systems and controls and compliance with anti-money laundering legislation applicable in its jurisdiction of establishment, jurisdiction of operations and the DIFC (including applicable UAE legislation) and RM AML Regime;

2) the day-to-day operation for compliance with the Member's anti-money laundering policies, procedures, systems and controls;

3) acting as the point of contact to receive internal suspicious transaction reports, taking the appropriate action and making the relevant notifications pursuant to anti money laundering legislation applicable in the DIFC (including applicable UAE legislation) and under the RM AML Regime. Such notifications shall include notifying Nasdaq Dubai and DFSA of all suspicious transactions relating to dealings on or connected with transactions on Nasdaq Dubai;

4) acting as the point of contact for money laundering issues;

5) responding promptly to any request for information made by Nasdaq Dubai, the DFSA and/or competent UAE authorities regarding money laundering issues; and

6) establishing and maintaining an appropriate anti-money laundering training programme and retaining records of employees attendance at such programmes.

2.2.7 A Member's anti-money laundering policies, procedures, systems and controls should be subject to periodic audit specifically with regard to testing its adequacy to meet the Nasdaq Dubai Rules.

2.2.8 The audit/testing may be conducted by a Member's own personnel not involved in the design or implementation of the policies, procedures, systems and controls or it may be done by a qualified third party.