مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

## ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM AND ILLEGAL ORGANISATIONS

# GUIDANCE FOR LICENSED EXCHANGE HOUSES

November 11, 2021

## TABLE OF CONTENTS

# 1. Introduction

## 1.1. Purpose

Article 44.11 of the *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 Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") Licensed Exchange Houses ("LEH") of their statutory obligations under the legal and regulatory framework in force in the UAE. It should be read in conjunction with the Chapter 16 of the Standards for the Regulations Regarding Licensing and Monitoring for Exchange Business, Version 1.20 of November 2021 amending Version 1.10 of February 2018 (*issued by Notice No. xx/2021 dated xx/xx/2021)*, the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 79/2019 dated 27/06/2019) and any amendments or updates thereof.[1] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LEH to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the Central Bank.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices and red flag indicators. These are not exhaustive and do not set limitations on the measures to be taken by LEH in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LEH should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LEH expected to demonstrate compliance with its requirements within one month from its coming into effect.

## 1.2. Applicability

Unless otherwise noted, this Guidance applies to all Exchange Houses that are licensed and supervised by the CBUAE.

## 1.3. Legal Basis

This Guidance builds upon the provisions of the following laws and regulations:

- Federal Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations ("AML-CFT Law)" and its amendment (Federal Decree Law

[1] Available at https://www.centralbank.ae/en/cbuae-amlcft.

No. (26) of 2021 amending certain provisions of Federal Decree Law No. 20 for 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations).

- Cabinet Decision No. (10) of 2019 concerning the Implementing Regulation of Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations ("AML-CFT Decision").
- Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council (UNSC) Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution ("Cabinet Decision 74").
- CBUAE Regulations regarding Licensing and Monitoring of Exchange Business issued in January 2014 ("the Regulations") issued by Notice 1/2014 dated 06/01/2014 and its amendment issued by Notice 269/2016 on 25/08/2016.
- Chapter 16 on AML/CFT Compliance of the Standards for the Regulations Regarding Licensing and Monitoring of Exchange Business, Version 1.20 of November 2021 amending Version 1.10 of February 2018 ("The Standards").

Furthermore, LEH may be guided by the FATF standards on AML/CFT, Guidance for a Risk Based Approach for Money or Value Transfer Services, and Report on Money Laundering through Money Remittance and Currency Exchange Providers.[2]

## 1.4. Definitions

**Beneficial Owner:** The 'Natural Person' who ultimately owns or exercises effective control, directly or indirectly, over a customer or the natural person on whose behalf a transaction is being conducted, or the natural person who exercises effective ultimate control over a legal person or legal arrangement.

**Exchange Business:** Shall mean: (1) Dealing in sale and purchase of foreign currencies and travelers cheques; (2) Executing remittance operations in local and foreign currencies; (3) Payment of wages through establishing a link to the operating system of "wages protection system" (WPS); and (4) Other business licensed by the CBUAE.

**Exchange House**: A juridical person licensed in accordance with the provisions of *Decretal Federal Law No. (14) of 2018 Regarding the Central Bank & Organization of Financial Institutions and Activities* to carry on money exchange activity, and conduct funds transfers within and outside the UAE, and any other businesses determined by the CBUAE.

**Politically Exposed Person (PEP):** natural persons who are or have been entrusted with a prominent public function in the UAE or any other foreign country such as heads of states or governments, senior politicians, senior government officials, judicial or military officials, senior executive managers of state-owned corporations, and senior officials of political parties, and persons who are, or have previously been, entrusted with the management of an international organization or any prominent function within such an organization; and the definition also includes the following:
1. Direct family members (of the PEP who are spouses, children, spouses of children, parents)

[2] FATF: Guidance-RBA-money-value-transfer-services.pdf (fatf-gafi.org); and Money laundering through money remittance and currency exchange providers (fatf-gafi.org)

2. Associates known to be close to the PEP, which include:
(a) Individuals having joint ownership rights in a legal person or arrangement or any other close business relationship with the PEP;
(b) Individuals having individual ownership rights in a legal person or arrangement established in favor of the PEP.

**Instant Money Transfer Service Provider:** A money remitting institution licensed and regulated by an appropriate Regulator in its home country who will have the necessary proprietary software applications and infrastructure to transfer funds instantly from an agent in one country to an agent in another country and/or domestically.

**Legal person**: Any entities other than natural persons that can establish in their own right a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, partnerships, or associations, along with similar entities.

**Legal arrangement**: A relationship established by means of a contract between two or more parties which does not result in the creation of a legal personality. Examples include trusts or other similar arrangements. Many legal arrangements allow for ownership, control, and enjoyment of funds to be divided between at least two different persons.

**Licensed Exchange House (LEH):** An Exchange House licensed by the CBUAE.

**Source of funds:** How the money, involved in the transaction, was originally derived or earned. Examples of source of funds are: salary, wages, inheritance, gratuity, end of service benefits, bank loan, income from businesses, sale of property, sale of land, sale of investments, etc. For verification of the source of funds, documents include but are not limited to salary slip, labor contract, court order, bank statements, etc.

# 2. Risks related to the Exchange Houses Sector

The FATF's Mutual Evaluation Report of the UAE issued in April 2020 stated that the Money or Value Transfer Services' sector (MVTS), including the Exchange Houses' sector, is weighted as highly important in terms of risk and materiality in the UAE. The inherent risk and materiality of these sectors has been notably increased by their exposure to cash transactions.

The Exchange Houses sector provides widely used financial services to diverse customer sectors. While the majority of its Exchange Business is legitimate in purpose, it can be abused to facilitate illegal activity, including terrorist financing, money laundering, and other type of criminal activity. The Exchange Houses sector may provide significant opportunities for criminals to move, conceal and eventually use the funds generated by their illegal activities, unless appropriate safeguards are in place. This is due to the simplicity and speed of transactions, worldwide reach and often cash-based nature of transactions. Importantly, money laundering and financing of terrorism (ML/FT) vulnerabilities also stem from the fact that Exchange Houses often carry out occasional transactions rather than establishing an ongoing formal relationship with their customers, which means that their understanding of the ML/FT risk associated with the customer may be limited.

Risks to the Exchange Houses sector also stem from generally uneven regulatory disparity, supervision and enforcement of the sector globally because Exchange Business often involves different jurisdictions. Criminals may seek to exploit differences in regulatory requirements in different jurisdictions or deficiencies in certain jurisdictions to move, structure and conceal their funds.

Exchange Houses may also potentially be abused by criminal groups and corrupt employees or agents co-operating with criminals, who may seek to own an Exchange House outright, or indirectly through an associate, or could seek to coerce employees through financial incentives in order to use the Exchange House to circumvent AML/CFT obligations and advance criminal schemes.

# 3. Regulation and Supervision of Exchange Houses

The Exchange Houses sector is regulated by the Regulations and the Standards issued by the CBUAE. For more details and information on AML/CFT compliance, please refer to *Chapter 16 of the Standards for the Regulations Regarding Licensing and Monitoring for Exchange Business, version 1.20 of November 2021 amending Version 1.10 of February 2018*. LEH are supervised by the CBUAE, who may examine the activities of the LEH at any time it deems appropriate to ensure proper compliance with their statutory obligations under the legal and regulatory framework in the UAE, or impose supervisory action or administrative and financial sanctions for violations. Similar to its all LFIs, the CBUAE applies the principle of proportionality in its supervision and enforcement process, whereby small LEH may demonstrate to the CBUAE that the objectives of the regulatory requirements are met without necessarily addressing all the specifics cited in the legal and regulatory framework in the UAE

# 4. AML/CFT Program for Licensed Exchange Houses

LEH must carefully design, document and effectively implement an AML/CFT Program in line with the provisions of the Standards, AML-CFT Law, and AML-CFT Decision. As per Paragraph 16.1 of the Standards, LEH must establish, maintain and regularly update effective, written, and risk-based AML/CFT programs designed to prevent LEH from being abused to facilitate ML/FT. When designing or updating their AML/CFT programs, the scope of the AML/CFT Program should be proportionate to the level of the risk posed by the LEH's size, scale, complexity, the nature and volume of its Exchange Business, the nature of its customer base, the business relationships it maintains, and the geographic areas in which it operates. For example, a large LEH with a high volume of Exchange Business with high-risk countries is expected to have an AML/CFT Program commensurate with its higher risk of possibly being abused to facilitate ML/FT. However, as all LEH are exposed to some degree of risk, they must perform their own assessments and design their AML/CFT programs in accordance with their overall risk profile in order to meet their statutory obligations.

**LEH should ensure the AML/CFT Program includes the following ten (10) essential components,** which are described in detail in the following sections:

- Risk assessment,
- Policies and procedures,
- Governance and the Compliance Officer,

- Customer due diligence,
- Transaction monitoring,
- Sanctions obligations and freezing without delay,
- Training,
- Independent audit,
- Record keeping requirements, and
- Managing employee risk.

## 4.1. Risk Assessment

As required by Article 4 of the AML-CFT Decision and Paragraph 16.2 of the Standards, LEH must identify, assess and understand the ML/FT risks associated with their businesses and perform an enterprise wide ML/FT risk assessment on a regular basis. It must develop a risk assessment in order to understand how and to what extent it is vulnerable to ML/FT, and help determine the nature and extent of AML/CFT resources necessary to mitigate and manage that risk.

The risk assessment creates the basis for the LEH's risk-based approach. LEH may utilize a variety of models or methodologies to analyze their risks. In general, the risk assessment process would entail the following six (6) steps:

| Step 1 | Step 2 | Step 3 | Step 4 | Step 5 | Step 6 |
|---|---|---|---|---|---|
| **Scope Determination** | **Risk Identification** | **Inherent Risk Assessment** | **Controls Evaluation** | **Residual Risk Assessment** | **Risk Mitigation** |
| Define in-scope processes | Assess the exposure to threats and vulnerabilities in order to identify risks | Assess the impact and likelihood of risks and assign inherent risk ratings | Identify and evaluate effectiveness of controls and identify weaknesses | Calculate Residual Risk (Inherent Risk Rating minus Controls Evaluation = Residual Risk Rating) | Develop and implement mitigation plans against risks that are above an acceptable level |

The nature and extent of any assessment of ML/FT risks must be appropriate to the nature, size, and complexity of the LEH's business. The risk assessment should cover all relevant factors including but not limited to:

- Customer risk;
- Products and services risk;
- Delivery channel risk;
- New technologies risk;
- Jurisdiction or geographic risk;
- Counterparty risk; and
- Other areas of risk.

As per Article 4.2 of the AML-CFT Decision as well as Paragraphs 16.2 and 16.3 of the Standards, the senior management of the LEH must be closely engaged in the risk assessment process and take

responsibility for conducting an appropriate assessment. It must review and approve at least on an annual basis the LEH's risk appetite statement, risk assessment methodology, and risk assessment findings. If an initial risk assessment assesses the LEH as higher risk, it may be necessary to conduct a more intensive assessment of certain areas of the LEH's operations. In assessing ML/FT risks, the LEH must have the following elements in place:

- Documented risk assessment methodology, procedures, and processes.
- Documented risk assessment findings, including determination of overall risk and specific risks, and mitigating measures to be applied to minimize the impact of risks.
- Written risk appetite statement that clearly identifies the acceptable level of risk.
- Appropriate mechanisms to provide information on risk assessments to the CBUAE when required.

The risk assessment must be regularly updated annually at a minimum as well as in response to major changes in the LEH's operations. The risk assessment process must also be fully aligned with the LEH's products, services, customers, and geographic locations, changes in the LEH's operations, appetite statement, the legal and regulatory framework in force in the UAE, and the guidance issued by the CBUAE. In addition, LEH may consult the the FATF *Guidance on the Risk-Based Approach for Money Services Businesses* and the *Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption* for more information on how to plan and perform comprehensive and appropriate risk assessments.[3] In tandem, the risk assessment findings should be used to inform the AML/CFT Program policies, procedures, internal controls, and training in order to effectively mitigate risks. The risk assessment should also inform the LEH's risk-based approach by directing an efficient allocation of AML/CFT risk management resources to the areas of greatest concern. The risk assessment findings should be provided to all business lines across the LEH, its senior management, and relevant employees.

### 4.1.1. *Customer Risk*

Under Article 4.1 of the AML-CFT Decision and Paragraph 16.2.3 of the Standards, LEH must identify, assess, understand, and mitigate the risk posed by their customers. Customer risk is a critical component of an institutional-level risk assessment because customers engaged in illicit activity can seek to exploit the LEH to facilitate ML/FT and other types of financial crimes. The customer risk assessment process is composed of the customer risk rating, and the assessment of the inherent risk of the customer base. It should be noted that these are closely related concepts, and that risk in the customer base depends in part on the customer risk rating.

#### 4.1.1.1. *Customer Risk Rating*

LEH should be able to determine whether a particular customer poses higher risk and the potential impact of any mitigating factors on that assessment. Such categorization may be due to the occupation, behavior, or activity of customers. Accordingly, the LEH should assess the risk of key customer elements in order to generate an overall customer rating. Generally, the list of elements includes but is not limited to the following:

- Customer's address and country.

[3] Available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf; and https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf.

- Type of customer (Domestic, foreign, company/corporate, cash-intensive business, etc.).
- Industry in which the customer does business.
- Anticipated transactional activities.
- Customer's source of wealth.
- ML/FT risk of the customer's industry
- The beneficial owners.
- Purpose of the relationship or transactional activities.

Below are some examples of risk factors that could be considered by the LEH:

- Customers conducting their business or transactions in an unusual manner.
- Customers who travel unexplained distances to locations to conduct transactions.
- Customers who are Politically Exposed Persons (PEPs) or their direct family members or known close associates and customers whose beneficial owner is a PEP.
- Customers involved in transactions that have no apparent ties to the destination country and with no reasonable explanations.
- Customers who have been the subject of legal proceedings in relation to proceeds-generating crimes known to the LEH.

#### 4.1.1.2. *Assessment of the Inherent Risk of the Customer Base*

In addition to assessing individual customers, LEH should assess the inherent ML/FT risk of the customer base overall.

1. **IDENTIFY**: LEH should identify categories or types of customers that pose elevated risks. Under Chapter 16 of the Standards, the categories identified will depend on the specific customer base of the LEH and may include but are not limited to: customer types like dealers in precious metals and stones (DPMS), customers that qualify as Designated Non-Financial Businesses and Professions (DNFBPs), cash-intensive businesses which are rated as high-risk[4], PEPs, and customers with ties to high risk jurisdictions. LEH should also include as a customer segment those customers who have been off-boarded or refused service due to ML/FT suspicions.
2. **ASSESS**: LEH should assign a risk rating (for example, low risk, medium risk, etc.) to each customer category or type identified above. In assessing the risk of each category or type, LEH should consider:
   - Guidance published by the FATF;
   - The potential exposure of customers in each category to illicit funds; and
   - The features of each customer type that make them useful to illicit actors.
3. **CALCULATE EXPOSURE**: The LEH should then determine its exposure to the customer categories or types identified and rated above. LEH should consider the proportion of their entire customer base that is made up of each category of customer, the proportion of all transactions carried out by each category of customer, and the total value of all transactions carried out by each customer as a proportion of the LEH's total transaction volume. The institutional risk assessment should also take into account the individual customer risk-ratings and the proportion of higher or lower risk customers within

[4] For more details and information, please refer to the CBUAE's *Guidance for Licensed Financial Institutions providing services to Cash-Intensive Businesses* available at https://www.centralbank.ae/en/cbuae-amlcft

that group. Where a LEH has large exposure to higher-risk customer types and to higher-risk customers as assessed by individual risk ratings, its overall inherent risk will generally be higher.

4. **DOCUMENT**: A LEH's approach to categorizing risk should be clearly documented. The LEH should keep detailed records of its assumptions, statistics used to complete this process, and the resulting analysis and outcomes.

### *4.1.2. Products and Services Risk*

Under Article 4.1 of the AML-CFT Decision and Paragraph 16.2.3 of the Standards, LEH must identify, assess, understand, and mitigate the risk posed by the products and services they offer. The products and services risk is a critical component of an institutional-level risk assessment because customers engaged in illicit activity can seek to exploit the LEH to facilitate ML/FT and other types of financial crimes.

1. **IDENTIFY**: LEH should identify the full list of products and services they offer.
2. **ASSESS**: LEH should assign a risk rating to each product type identified above. Determining the risk of products and services should include a consideration of their characteristics and attributes and could include factors such as:
    - Products or services that may inherently favor anonymity, or products that can readily cross international borders, such as cash, online money transfers, stored value cards, money orders and international money transfers by mobile phone.
    - Products or services that have a very high or no transaction limit.
    - The global reach of the product or service offered.
    - The complexity of the product or service offered.
    - Products or services that permit the exchange of cash for a negotiable instrument, such as a stored value card or a money order.
3. **CALCULATE EXPOSURE**: The LEH should consider what proportion of its total products and services, and of total transactional activity, is associated with higher and lower-risk products and services. Where a LEH has large exposure to higher-risk products and services, its overall inherent risk will generally be higher.
4. **DOCUMENT**: A LEH's approach to categorizing risk should be clearly documented. The LEH should keep detailed records of its assumptions, statistics used to complete this process, and the resulting analysis and outcomes.

### *4.1.3. Delivery Channel Risk*

Under Article 4.1 of the AML-CFT Decision and Paragraph 16.2.3 of the Standards, LEH must identify, assess, understand, and mitigate the risk presented by the delivery channels they use. Some delivery channels can increase ML/FT risk because they increase the risk that the LEH does not truly know or understand the identity and activities of the customer.

1. **IDENTIFY**: The LEH should identify the delivery channels that they use to provide their products and services to customers. These may include, for example: face-to-face; via a website; via an introducer or other third party; and other methods.

2. **ASSESS:** The LEH should assign an inherent risk rating to the delivery channels identified. The rating should take into consideration the characteristics and attributes of these delivery channels that make them more susceptible to abuse by illicit actors, and could include factors such as whether the delivery channel makes it more difficult to observe the customer's behavior or to be certain that the person transacting is in fact the identified customer, allows for faster transactions, or involves reliance on a third party.
3. **CALCULATE EXPOSURE**: The LEH should then determine what proportion of its transactional activity involves each delivery channel, both by volume and value. Where a LEH delivers a large proportion of its products or services via higher-risk delivery channels, its overall risk is likely to be higher as well.
4. **DOCUMENT**: A LEH's approach to categorizing risk should be clearly documented. The LEH should keep detailed records of its assumptions, statistics used to complete this process, and the resulting analysis and outcomes.

### *4.1.4. New Technologies Risk*

Under Article 23 of the AML-CFT Decision and Paragraphs 16.2.3 and 16.2.7 of the Standards, LEH must identify, assess, understand, and mitigate the ML/FT risk to which they may be exposed by new technologies, including new delivery mechanisms and the use of new or developing technologies for both new and existing products. LEH must undertake the risk assessment **prior to obtaining approval from the CBUAE to launch or use such products, services, and technologies if applicable**.

1. **IDENTIFY:** LEH should identify the new technologies they plan to introduce. New technologies can involve new or modified products and services and also new or modified delivery channels.
2. **ASSESS**: The LEH should assign an inherent risk to each proposed new technology. Determining the risk of new technologies should include a consideration of their characteristics and attributes. In addition to the factors listed above under sections 4.1.2 and 4.1.3, this could include factors such as features of the technology that promote anonymity or obstruct access to transaction or customer information, a history of ML/FT abuse of the technology, the inherent risk of the target customer and market segments that are projected to use the new technology, and expected growth in use of the technology.
3. **CALCULATE EXPOSURE**: The LEH should consider the projected or expected volume of transactional activity associated with the new technology and follow the procedure described in sections 4.1.2 and 4.1.3 above.
4. **DOCUMENT**: A LEH's approach to categorizing risk should be clearly documented. The LEH should keep detailed records of its assumptions, statistics used to complete this process, and the resulting analysis and outcomes.

### *4.1.5. Jurisdiction or Geographic Risk*

Under Article 4.1 of the AML-CFT Decision and Paragraph 16.2.3 of the Standards, LEH must identify, assess, understand, and mitigate their jurisdiction or geographic ML/FT risk.

1. **IDENTIFY**: LEH should identify the geographic footprint of their operations, which should include:
    - The jurisdictions in which they have locations, including domestic locations;

- The jurisdictions in which their customers are resident or of which they are nationals (for Non-Resident Customers only);
- The jurisdictions to which they send remittances to or receive remittances from; and
- The jurisdictions to or from which they import or export foreign currency.

LEH need not include every single jurisdiction to or from which they send or receive remittances or with which their customers have ties in the risk assessment, but should at least include the jurisdictions to which they have regular or routine exposure.

2. **ASSESS**: The LEH should assign each jurisdiction identified above an inherent risk-rating, based on the degree of ML/FT risk present in that jurisdiction. The LEH is strongly encouraged to develop its own country risk model that takes into consideration any publications issued by the National Anti-Money Laundering and Combating the Financing of Terrorism and financing of Illegal Organizations Committee (NAMLCFTC)[5], the UAE Financial Intelligence Unit (FIU), the FATF lists of High-Risk Jurisdictions subject to a Call for Action and Jurisdictions under Increased Monitoring,[6] as well as the Organization for Economic Cooperation and Development (OECD) list of jurisdictions classified as uncooperative tax havens.[7] The LEH should also consider whether a jurisdiction:

   - Has been identified by credible sources as providing an environment conducive to funding or supporting terrorist activities or that have designated terrorist organizations operating within them.
   - Has been identified by credible sources as having significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling.
   - Is subject to sanctions, embargoes or similar measures issued by international organizations such as the United Nations.
   - Has been identified by credible sources as having weak governance/law enforcement/regulatory regimes, including countries identified by the FATF as having weak AML/CFT regimes [8], for which financial institutions should give special attention to business relationships and transactions.

   Finally, the LEH should take into consideration its own knowledge and experiences, such as the number of Suspicious Transaction Reports (STR) or Suspicious Activity reports (SAR) filed that involve each jurisdiction.

3. **CALCULATE EXPOSURE**: The LEH should consider what proportion of its total customer base and transactional activity, by volume and value, is associated with or linked to higher or lower-risk jurisdictions. Based on its documented understanding of the risks, the LEH may decide to weigh its exposure so that a cross-border transaction to a beneficiary in a high-risk jurisdiction has a greater impact than, for example, a domestic transaction between two UAE residents where one party is a citizen of a high-risk jurisdiction. Where a LEH has large exposure to higher-risk jurisdictions, its overall inherent risk will generally be higher.

[5] Available at: https://www.namlcftc.gov.ae/en/high-risk-countries.php
[6] Available at: https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)
[7] Available at: http://www.oecd.org/ctp/harmful/theoecdissuesthelistofunco-operativetaxhavens.htm.
[8] See footnote 12

4. **DOCUMENT:** A LEH's approach to categorizing risk should be clearly documented. The LEH should keep detailed records of its assumptions, statistics used to complete this process, and the resulting analysis and outcomes.

### *4.1.6. Counterparty Risk*

As required by Article 25 of the AML-CFT Decision and Paragraph 16.2.3 of the Standards LEH must identify, assess, understand, and mitigate counterparty risk prior to establishing business relationships with counterparties, and on an ongoing basis once the relationship is established. Counterparty relationships include the following types:

- Domestic and Foreign correspondent banking arrangements, such as those with banks, exchange houses, or any other financial institutions for the purpose of money transfer services.
- Money transfer arrangements with instant money transfer service providers.
- Hedging arrangements with local or foreign institutions.
- Arrangements to import or export banknotes from/to foreign institutions, such as Banks, exchange houses, or other financial institutions outside the UAE.
- Arrangements with local or foreign entities to offer special products/services.

1. **IDENTIFY**: LEH should identify all counterparties that fit the description above, including with affiliates and other members of the same group.
2. **ASSESS**: The LEH should assign an inherent risk rating to each counterparty. The determination of the counterparty's risk should include a consideration of all characteristics and attributes that make the counterparty more or less susceptible to abuse by illicit actors, as well as characteristics and features of the counterparty relationship that could increase or decrease risk. This could include for example:

    - The risk of the country in which a counterparty is registered;
    - The products and services it offers and the risks of the counterparty's customer base overall;
    - Its reputation in the sector and any adverse media;
    - Its ownership (including links to PEPs or persons associated with adverse media);
    - The counterparty's experience in this sector and its overall sophistication;
    - The quality and intensiveness of the counterparty's AML/CFT program, including whether the program's requirements are consistent with minimum requirements imposed in LEH by the legal and regulatory framework in force in the UAE;
    - The quality and rigor of supervision applied to the counterparty;
    - Any regulatory or criminal enforcement actions taken against the counterparty; and
    - The nature and purpose of the counterparty relationship, including the risk of the products and services involved and the types of customers who use the relationship.

3. **CALCULATE EXPOSURE**: LEH should determine the proportion of counterparties that are rated higher risk, both in terms of actual numbers and in terms of the volume and value of the transactions involving that counterparty. Because counterparty relationships may involve rapid, large changes in the volume of transactions, LEH should continuously monitor their exposure to counterparties and update their risk assessment whenever exposure changes substantially.

4. **DOCUMENT**: A LEH's approach to categorizing risk should be clearly documented. The LEH should keep detailed records of its assumptions, statistics used to complete this process, and the resulting analysis and outcomes.

### *4.1.7. Other Areas of Risk*

In addition to the ML/FT risks discussed in this section, LEH may be exposed to other areas of illicit finance risk, including sanctions and proliferation financing. The LEH may choose to include these risk domains in its AML/CFT assessment as long as the resulting assessment gives appropriate space and attention to ML/FT risk. Given the evolving nature of ML/FT risks, LEH may also choose to assess their ML/FT risk in additional categories to those discussed above (although they must always address at least the categories covered in this section).

Under Article 4.1(b) of the AML-CFT Decision and Paragraph 16.2.5 of the Standards, LEH must thoroughly document their risk assessment process so that they can fully explain and justify their assessment methodology.

## 4.2. Policies and Procedures

As required by Article 4.2.a) of the AML-CFT Decision and Paragraph 16.3 of the Standards, LEH must establish and implement comprehensive and documented AML/CFT policies and procedures to enable them to effectively manage and mitigate the risks they have identified. Under Paragraph 16.3.6 of The Standards, these must be approved by the Manager in Charge, the Compliance Officer, and the Board of Directors (or Owner/Partners where there is no Board of Directors). They must be reviewed and updated annually at a minimum to ensure that they are consistent with statutory obligations and other international best practices, and effective in mitigating existing as well as emerging ML/FT risks as per Paragraph 16.3.7 of the Standards. Policies and procedures should at a minimum:

- Be commensurate with the nature, size, and complexity of the LEH's operations.
- Outline the AML/CFT Program.
- Be consistently implemented across all branches, subsidiaries and affiliated entities in which the LEH holds a majority interest.
- Capture the LEH's day-to-day operations and processes.
- Clearly define the roles and the day-to-day responsibilities of the Manager in Charge, Compliance Officer, Compliance Committee and employees in relation to AML/CFT compliance as well as the ones of the Board of Directors (or Owner/Partners where there is no Board of Directors) in relation to implementing a robust compliance program across the business of the LEH.
- Enable the LEH to clearly and effectively identify, escalate, and report suspicious transactions and activities.
- Require enhanced due diligence to be conducted on all customers and transactions that are assessed to be high-risk.
- Prohibit employees from, directly or indirectly, informing the customer or any third party that their transactions are subject to monitoring or under investigation or have been reported to the FIU as suspicious transactions.
- Contain sufficient detail of their record keeping obligations.

Policies and procedures should be clearly communicated to all relevant employees. They should be easy to follow and be designed to support the compliant and effective functioning of the AML/CFT program and prevent employees from engaging in misconduct.

## 4.3. Governance and Compliance Officer

The core of an effective risk-based program is an appropriately experienced AML/CFT Compliance Officer who understands the LEH's risks and obligations and who has the resources and autonomy necessary to ensure that the LEH's program is effective. As per Article 21 of the AML-CFT Decision and Paragraph 16.4 of the Standards, the LEH must appoint a Compliance Officer who is responsible for day-to-day compliance with the legal and regulatory framework in the UAE and the management of the AML/CFT Program. The role of Compliance Officer must be limited to tasks related to AML/CFT compliance and not be combined with any other functions of the LEH to avoid conflict of interest from multiple roles. Furthermore, as per Paragraphs 16.5 and 6.9.3 of the Standards, the LEH must further appoint an Alternate Compliance Officer to strengthen the AML/CFT Program as well as establish and maintain a Compliance Committee to provide additional oversight of the AML/CFT program. Chapter 6 of the Standards refers to Corporate Governance as the mechanisms and processes by which the LEH is managed, controlled and directed. For more details and information please refer to the relevant section in the Standards.

## 4.4. Customer Due Diligence

The goal of the CDD process is to ensure that LEH understand who their customer is and the purpose for which the customer will use the LEH's services**. Where a LEH cannot satisfy itself that it understands a customer, then it must not accept the customer. If there is an existing business relationship, the LEH should not continue it.** LEH should also consider filing an STR, SAR or other report types to the FIU as discussed in section 5 below. This guidance is not an exhaustive list of CDD obligations and LEH should consult the legal and regulatory framework in force in the UAE for the measures to be taken.

Under Article 8 of AML-CFT Decision, LEHs are required to identify and verify the identity of all customers. In particular, when verifying the Emirates ID card (either physically or by way of digital or e-KYC solutions) the LEH must use the online validation gateway of the Federal Authority for Identity & Citizenship, the UAE-Pass Application, or other UAE Government supported solutions, and keep a copy of the Emirates ID and its digital verification record. Where acceptable IDs other than the Emirates ID are used in the KYC process, a copy must be physically obtained from the original ID and certified as "Original Sighted and Verified" by the employee who carries out the CDD process.

As required by Paragraph 16.7 of the Standards, LEH must implement a strong Know Your Customer ("KYC") process that is based on clear and comprehensive written policies and procedures. Implementation of an effective KYC process is an essential cornerstone of a LEH's AML/CFT Program and is necessary in order to:

- Understand who LEH's customers and counterparties are.
- Detect suspicious activity or transactions in a timely manner.
- Promote safe and sound business practices.
- Minimize the risk that the LEH is abused by illicit actors.
- Reduce the risk of processing transactions when the customer is involved in criminal activity.

- Protect the reputation of the LEH.
- Comply with statutory obligations.

The KYC process must be risk-based and, as such, the KYC measures applied must be commensurate with the ML/FT risks associated with their customers or transactions. Accordingly, Paragraph 16.7.3 of the Standards requires three types of KYC processes that must be applied depending on the customer's risk and the nature of the transaction and customer. These are:

- Customer Identification (CID);
- Customer Due Diligence (CDD); and
- Enhanced Due Diligence (EDD).

**Please refer to the table below on when to use each KYC measure and to refer to the respective paragraphs in the Standards for the detailed requirements:**

| **Customer Type** | **Customer Activity** | **Value of Transaction** | **Preventive Measure Required** | **Paragraph in** the Standards, Version 1.20 |
|---|---|---|---|---|
| Natural Persons | Currency Exchange | Equal to or greater than AED 3,500 and less than AED 35,000 | CID | 16.8 |
| | | Equal to or greater than AED 35,000 and less than AED 55,000 within a 90-day period | CID **and** CDD | 16.8<br>16.9 |
| | | Equal to or greater than AED 55,000 within a 90-day period | CID, CDD, **and** EDD | 16.8<br>16.9<br>16.10 |
| | Money Transfer | Any value less than AED 55,000 | CID **and** CDD | 16.8<br>16.9 |
| | | Equal to or greater than AED 55,000 within a 45-day period | CID, CDD, **and** EDD | 16.8<br>16.9<br>16.10 |
| All Legal Persons or Arrangements | Any Activity | Any Value | CDD **and** EDD | 16.11 |
| Counterparty Relationships | Any Activity | Any Value | CDD **and** EDD | 16.11.8 to 16.11.12<br>16.11.2 |
| PEPs | Any Activity | Any Value | CID, CDD, **and** EDD | 16.13 |
| DNFBPs/DPMS | Any Activity | Any Value | CID (if the customer is a natural person), CDD, **and** EDD | 16.14/16.15 |

| | | | | |
|---|---|---|---|---|
| High-Risk Natural Persons | Any Activity | Any Value | CID,<br>CDD, **and**<br>EDD | 16.16<br>16.8,<br>16.9<br>16.10 |
| High-Risk circumstances | Any Activity | Any Value | CID (if the customer is a natural person),<br>CDD, **and**<br>EDD | 16.16<br>16.8,<br>16.9<br>16.10/11 |
| Third Party Transactions | Any Activity | Any Value | CID (if the customer is a natural person),<br>CDD **and**<br>EDD | 16.20<br>16.8,<br>16.9<br>16.10/11 |

### *4.4.1. Ongoing Monitoring*

Under Article 7 of the AML-CFT Decision, LEH are required to ensure that the documents, data or information obtained under CDD measures are up-to-date and appropriate by reviewing the records, particularly those of high-risk customer categories. Ongoing monitoring allows the LEH to ensure that the Exchange Business is being used in accordance with the customer or relationship profile developed through KYC during onboarding, and that transactions are normal, reasonable, and legitimate.

As per Paragraphs 16.9.11 and 16.11.7 of the Standards, where the customer is a natural person (when CDD must be applied) or a legal person or arrangement, the customer profile must be reviewed and updated either annually, or at least upon the expiry of the ID, the trade license or the ID of any person authorized to make transactions on behalf of the customer, whichever comes first. At this time, the LEH must conduct ongoing monitoring on the customer which must consist of the following:

- The original ID must be verified (in accordance with Paragraphs 16.8.3, 16.9.6 and 16.9.7) and its copy must be held in the records during the review of a customer profile;
- CDD (and, where appropriate, EDD) must be repeated and the customer profile updated, including the information required under Paragraph 16.9.4 or 16.11.2 of this Chapter.
- CDD and EDD must also be repeated whenever there is a change in the profile of the customer;
- LEH must scrutinize the transactions concluded by a customer to ensure that transactions are consistent with its knowledge of the customer, the customer's business, risk profile, the source of funds and where necessary, source of the customer's wealth; and
- LEH must review transaction monitoring results for the customer to determine whether any STR/SARs or other reports have been filed or whether the customer's behavior has generated alerts.

Unless otherwise required, such as in the cases above mentioned, LEH should update the KYC information on customers and counterparties on a risk-based schedule, with KYC on higher-risk customers being updated more frequently. KYC updates should include a refresh of all elements of initial KYC, and in particular must ascertain whether:

- The customer/counterparty's beneficial owners remain the same.

- The customer continues to have an active status with the LEH Point of Sale system.
- The customer/counterparty is domiciled in the same jurisdiction.
- The customer/counterparty is engaged in the same type of business, and in the same geographies.
- The customer/counterparty's transactions continue to fit its profile and business, and are consistent with the business the customer expected to engage in when the business relationship was established, or the business that the LEH expected to engage in when it established the counterparty relationship.

If any of the above characteristics have changed, the LEH should risk-rate the customer/counterparty again.

Furthermore, LEH should conduct EDD when the revised risk rating demands it or if the customer/counterparty's history of transactions is not consistent with its profile and the expectations established at account opening. In particular, if the customer/counterparty's transactions/behavior have resulted in the filing of an STR/SAR with the FIU, the LEH should review the customer/counterparty profile and the activity that led to the report and make a determination as to whether the risk rating should be raised or the relationship should be terminated. LEH may consider requiring that the customer/counterparty update them as to any changes in its beneficial ownership. Even if this requirement is in place, however, LEH must not rely on the customer/counterparty to notify it of a change, but must still update KYC on a schedule appropriate to the customer's risk rating.

## 4.5. Transaction Monitoring

As required by Article 7 of the AML-CFT Decision and Paragraph 16.24 of the Standards, LEH must continuously monitor all their transactions to ensure that the transactions conducted are consistent with the information they have about the customer, their type of activity and the risks they pose, including, when necessary, the source of funds. Transaction monitoring systems allow the LEH to monitor the transactions made by their customers in real-time and/or on a daily basis. All LEH should have a form of transaction monitoring system in place in order to monitor for any suspicious transactions to and from customers. **Failure to have such a system in place may not only cost a LEH its reputation, but also lead to large fines and other penalties.**

Transaction monitoring is distinct from the ongoing monitoring discussed in section 4.4.1. Both are required, but the purpose of transaction monitoring is not primarily to update the customer risk profile but to detect and investigate transactions that may need to be reported to the FIU because they are potentially related to illicit activity. While CDD review (as discussed in section 4.4.1) may take place once a year, transaction monitoring occurs in real time and is thus able to support prompt reporting to the FIU after the transaction takes place.

Under Article 4.2 (a) of the AML-CFT Decision and Paragraph 16.24.1 of the Standards, Transaction monitoring must be commensurate with the risk posed by the LEH's size, scale, complexity, the nature and volume of its Exchange Business, the nature of its customer base, and the geographic areas in which it operates. The transaction monitoring system used by a LEH, whether automated or manual, must be able to flag unusual movements of funds or transactions for further analysis. Rules and parameters must take account of ML/FT typologies in the Exchange Houses sector.

When the monitoring system generates an alert, it must be investigated and either escalated or otherwise dispositioned in a timely fashion in order to support prompt reporting to the FIU. Transaction monitoring

systems should create an audit trail of all activity related to alert generation, investigation, and disposition to have a clear understanding of the activity, and potentially report it to the relevant authorities.

For more details and information, please refer to the *CBUAE Guidance for Licensed Financial Institutions on Transaction Monitoring Screening and Sanction screening*[9].

### *4.5.1. Indicative Risk Factors Associated with Transactions*

The following is an indicative and non-exhaustive list of risk factors associated with transactions[10].

- **Customer's behavior at point of origination:**
  - Customer structures transaction in an apparent attempt to break up amounts to stay under any applicable CDD threshold to avoid reporting or other requirements.
  - Customer attempts a transaction, but given he or she would likely be subject to the CDD monitoring, cancels transaction to avoid reporting or other requirements.
  - Transaction is unnecessarily complex with no apparent business or lawful purpose.
  - Number or value of transactions is inconsistent with financial standing or occupation, or outside the normal course of business of the customer in light of the information provided by the customer when conducting the transaction or during subsequent contact.
  - Customer offers a bribe or a tip, or is willing to pay unusual fees to have transactions conducted.
  - Customer has vague knowledge about amount of money involved in the transaction.
  - Customer makes unusual enquiries, threatens or tries to convince employees to avoid reporting.
  - Customer sends money internationally and then expects to receive an equal incoming transfer or vice versa.
  - Customer transfers money to illegal online gambling sites. Email addresses containing gambling references or transfers to countries with large numbers of internet gambling sites.
  - Customer wires money to higher-risk jurisdiction/country/corridor.
  - Customer transfers money to claim lottery or prize winnings
  - Customer transfers money to someone met only online or appears to have no familial relationship with the receiver and no explanation forthcoming for the transfer.

- **Activity detected during monitoring** (in many of these scenarios the customer's activity may be apparent both during point-of-sale interaction and back-end transaction monitoring):
  - Transfers to the same person from different individuals or to different persons from the same individual with no reasonable explanation.
  - Unusually large aggregate wire transfers or high volume or frequency of transactions with no logical or apparent reason.
  - Customer uses aliases, nominees or a variety of different addresses.
  - Customers whose concentration ratio of transfers made to a jurisdiction is notably higher than what is to be expected considering overall customer base.
  - Customer transfers/receives funds from persons involved in criminal activities as per the information available.

[9] Available at https://www.centralbank.ae/en/cbuae-amlcft.
[10] FATF: Guidance-RBA-money-value-transfer-services.pdf (fatf-gafi.org)

- A network of customers using shared contact information (such as address, telephone or e-mail) where such sharing is not normal or reasonably justifiable.

- **Transactions received:**
  - Transactions that are not accompanied by the required originator or beneficiary information.
  - Additional customer or transactional information was requested from an ordering counterparty but not received.
  - Large number of transactions received at once or over a certain period of time which do not seem to match the recipient's usual past pattern.

## 4.6. Sanctions Obligations and Freezing Without Delay

Article 16.1 of the AML-CFT Law and Article 60 of the AML-CFT Decision require LEH to promptly apply directives issued by the Competent Authorities of the UAE for implementing the decisions issued by the United Nations Security Council under Chapter VII of the Charter of the United Nations ("UN"). In furtherance of this requirement, the Cabinet Decision 74 sets out the legal and regulatory framework in the UAE regarding Targeted Financial Sanctions ("TFS").

For more information and details on their obligations in relation to their sanctions obligations LEH should consult Paragraph 16.25 of the Standards; the Executive Office of the Committee for Goods and Materials Subjected to Import and Export Control's "*Guidance on Targeted Financial Sanctions for Financial Institutions and designated non-financial business and professions*"; the "*CBUAE Guidance for Licensed Financial Institutions on the Implementation of Targeted Financial Sanctions*" as well as the "*CBUAE Guidance for Licensed Financial institutions on Transaction Monitoring Screening and Sanctions screening*"[11].

Furthermore, LEH must sign up for the Integrated Enquiries Management System (IEMS) introduced by the FIU to automate and facilitate the execution process of requests for information, implementing decisions of public prosecutions and any other type of ML/FT requests. Via this system, the FIU can make requests to all LFIs simultaneously with the goal of processing requests and providing results to Law Enforcement Agencies more efficiently. For more information, LEH should consult the IEMS User Guide published by FIU[12].

## 4.7. Training

As per Paragraph 16.23 of the Standards LEH must provide comprehensive AML/CFT compliance training to all employees. The effective application of AML/CFT policies and procedures depends on the employees understanding not only of the processes they are required to follow, but also the risks these processes are designed to mitigate, and the possible consequences of those risks. Employees should remain abreast on an ongoing basis of emerging ML/FT typologies and new internal and external risks. The AML/CFT compliance training should be relevant to the LEH's ML/FT risks, business activities and up to date with the latest legal and regulatory obligations and internal controls. It should be tailored to particular lines of business within the LEH, equipping employees with a sound understanding of specialized ML/FT risks they

[11] Available at: https://www.centralbank.ae/en/cbuae-amlcft
[12] Available at: https://www.uaefiu.gov.ae/media/jtdnttby/integrated-enquiry-management-system.pdf

are likely to face, and their obligations in relation to those risks and must be provided to all new employees within thirty (30) calendar days from the date of joining. Thereafter, refresher training must be provided to all employees at regular intervals depending on the ML/FT risk exposure of each employee; for example, employees who deal directly with customers, products or services must be trained annually at a minimum. Refresher training must also be provided whenever there are changes in the legal and regulatory framework in force in the UAE or the LEH's AML policy/procedures. Furthermore, the AML/CFT compliance training should be provided to relevant employees upon learning of a confirmed negative risk assessment result or audit finding, or other deficiency pertaining to the AML/CFT Program. Evidence for all trainings conducted must be retained for inspection by the CBUAE.

## 4.8. Independent Audit

The independent audit process helps the LEH assess the effectiveness and adequacy of its current processes, including by assessing the adequacy of the AML/CFT Program and checking for any inconsistencies between the policy and procedures and day-to-day operations in order to identify any weaknesses and deficiencies. Independent auditing must be undertaken regularly to review and assess the effectiveness of the AML/CFT compliance policies, procedures, systems and controls, and their compliance with the LEH's obligations. As per Paragraph 16.31.1 of the Standards, the Compliance Officer's function must undergo regular audit by the LEH's internal audit department. In addition, under Paragraph 16.31.2 of the Standards, "agreed-upon procedures" for the review of the AML/CFT Compliance function must be performed by external auditors annually.

The independent audits, whether internal or external, should be undertaken by skilled and competent auditors. The internal audit department should be resourced with skilled and competent employees that understand the AML/CFT Program of the LEH. The audit should be commensurate to the level and sophistication of the LEH, and be updated to account for changes in risk assessments and the legal and regulatory framework in force in the UAE. The internal audit function should be accountable to the Board of Directors (or the Owner/Partners if there is no Board of Directors), independent of the audited activities and functions, and have sufficient authority, skills, expertise, and resources within the organization.

## 4.9. Record Keeping Requirements

Under Article 24 of the AML-CFT Decision, LEH must retain all records, documents, data and statistics for all transactions for a minimum period of five (5) years from the date of completion of the transaction or termination of the business relationship or from the closing date of the account. Records must be maintained in an organized manner so as to permit data analysis and, where relevant, the tracking of financial transactions. Records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. For more details and information please refer to paragraph 16.29 of the Standards.

## 4.10. Managing Employee Risk

As per Paragraphs 8.2 and 16.22 of the Standards, the LEH must implement an appropriate recruitment and Know Your Employee ("KYE") process for hiring employees and confirm the background of applicants prior to placing them in employment. The level of vetting procedures applied should reflect the ML/FT risks to which individual employees are exposed in their assigned roles. The LEH should be aware of potential

conflicts of interest for employees with AML/CFT responsibilities and should act to reduce or manage such conflicts of interest.

Furthermore, under Paragraph 16.28 of the Standards, the LEH must watch out for its employee's behavior and be aware of possible indicators of illicit behavior displayed by employees, such as:

- An employee whose lifestyle cannot be supported by his/her salary, which may indicate receipt of tips or bribes.
- An employee who is reluctant to take a vacation, which may indicate they have consented or are being forced to provide services to customers in violation of the law or company policy.
- An employee who is associated with an unusually large number of transactions or a transaction in an unusually large amount, which may indicate they have consented or are being forced to provide services to customers in violation of the law or company policy.

# 5. Reporting Obligations

## 5.1. Reporting to the CBUAE

As per Paragraph 4.21 of the Standards, LEH must submit reports to the CBUAE, which may be updated from time to time in terms of the frequency and form of submission and their deadline. For the submission of periodical returns/reports via the online system, the LEH must obtain access to the CBUAE reporting portals, such as its Integrated Regulatory Reporting System, Remittance Reporting System and/or other applicable system.

## 5.2. Reporting to the FIU

All LEH should have procedures and systems in place to ensure that suspicious activity is reported to authorities in an appropriate and timely manner. LEH must take into account all information from both the ordering and beneficiary sides in order to determine whether an STR or SAR is to be filed.

As required by Article 15 of AML-CFT Law and Article 17 of AML-CFT Decision, LEH must file without any delay an STR or SAR or other report types with the FIU using the "goAML" portal when they have reasonable grounds to suspect that a transaction, attempted transaction, or funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime. Under Article 24 of the AML-CFT Law, any person, including a LEH or their managers and employees, who violates on purpose or by gross negligence their statutory obligation to report a suspicion of money laundering and related predicate offences, financing of terrorism or illegal organisations is liable of the following sanctions:

- Imprisonment and fine of no less than AED100,000 and no more than AED1,000,000; or
- Any of these two sanctions (i.e. imprisonment or fine of no less than AED100,000 and no more than AED1,000,000).

For more details and information, please refer to Paragraph 16.27 of the Standards as well as the "*CBUAE Guidance for Licensed Financial Institutions on Suspicious Transaction Reporting*" [13].

# 6. Prohibition of Tipping Off

Under Article 25 of AML-CFT Law, anyone who notifies or warns a person or reveals any transaction under review in relation to suspicious transactions or being investigated by the competent authorities is punishable by a penalty of imprisonment for no less than six months and/or a fine of no less than AED 100,000 and no more than AED 500,000. Any such action is known as "tipping off." As per Paragraph 16.27 of the Standards, the prohibition on tipping off means that the LEH or its employees must not inform customers or any persons or third parties, either directly or indirectly, that their transactions are subject to monitoring, under investigation or have been reported to the FIU as suspicious transactions. The Compliance Officer should ensure that all employees of the LEH are aware of the consequences of tipping off. Sufficient AML/CFT training should be provided to all employees to ensure that they understand what constitutes tipping off and how to avoid it.

[13] Available at: https://www.centralbank.ae/en/cbuae-amlcft

# Annex1 – Synopsis of the Guidance

| | | |
|---|---|---|
| **Purpose of this Guidance** | **Purpose** | The purpose of this Guidance is to assist the understanding of risks and effective performance by the Licensed Exchange Houses ("LEH") of their AML/CFT statutory obligations. The FATF's Mutual Evaluation Report of the UAE issued in April 2020 stated that the Money or Value Transfer Services' sector, including the Exchange Houses' sector, is weighted as highly important in terms of risk and materiality in the UAE. The inherent risk and materiality of these sectors has been notably increased by their exposure to cash transactions. |
| | **Applicability** | This Guidance applies to all Exchange Houses that are licensed and supervised by the CBUAE. |
| **Risks Related to the Exchange House Sector** | The Exchange House sector provides widely used financial services to diverse customer sectors. While the majority of its Exchange Business is legitimate in purpose, it can be abused to facilitate illegal activity, including terrorist financing, money laundering, and other type of criminal activity. This is due to the simplicity and speed of transactions, worldwide reach, global regulatory disparity and often cash-based nature of transactions. Exchange Houses may also potentially be abused by criminal groups and corrupt employees or agents co-operating with criminals, who may seek to own an Exchange House outright, or indirectly through an associate or could seek to coerce employees through financial incentives. | |
| **Regulation and Supervision of Exchange Houses** | The Exchange Houses sector is regulated by the Regulations and the Standards issued by the CBUAE. For more detail and information, please refer to *Chapter 16 on AML/CFT Compliance of the Standards for the Regulations Regarding Licensing and Monitoring of Exchange Business* (Version 1.20 of November 2021 amending Version 1.10 of February 2018 ("The Standards")). LEH are supervised by the CBUAE, which may examine the activities of the LEH at any time it deems appropriate to ensure proper compliance with their statutory obligations under the legal and regulatory framework in the UAE, or impose supervisory action or administrative and financial sanctions for violations. | |
| **AML/CFT Compliance Program for LEH** | **AML/CFT Program** | LEH must carefully design, document and effectively implement an AML/CFT Program in line with the provisions of the Standards, AML-CFT Law, and AML-CFT Decision. When designing or updating their AML/CFT programs, the scope of the AML/CFT Program should be proportionate to the level of the risk posed by the LEH's size, scale, complexity, the nature and volume of its Exchange Business, the nature of its customer base, the business relationships it maintains, and the geographic areas in which it operates. |
| | **Risk Assessment** | LEH must develop a risk assessment in order to understand how and to what extent it is vulnerable to ML/TF, and help determine the nature and extent of AML/CFT resources necessary to mitigate and manage that risk, which should cover all relevant factors including but not limited to:<br>• Customer risk;<br>• Products and services risk;<br>• Delivery channel risk;<br>• New technologies risk;<br>• Jurisdiction or geographic risk;<br>• Counterparty risk; and<br>• Other areas of risk. |
| | **Policies and Procedures** | LEH must establish and implement comprehensive and documented AML/CFT policies and procedures to enable them to effectively manage and mitigate the risks identified. They must be approved, reviewed and updated, annually at a minimum, to ensure that they are consistent with the legal and regulatory framework in the UAE and other international best practices, and effective in mitigating existing as well as emerging ML/FT risks. |
| | **Governance and the Compliance Officer** | The core of an effective risk-based program is an appropriately experienced AML/CFT Compliance Officer who understands the LEH's risks and obligations and who has the resources and autonomy necessary to ensure that the LEH's program is effective. The role of Compliance Officer must be limited to tasks related to AML/CFT compliance and not be combined with any other functions of the LEH to avoid conflict of interest from multiple roles. The LEH must also appoint an Alternate Compliance Officer. |

| | | |
|---|---|---|
| **AML/CFT Program (cont'd)** | **Customer Due Diligence and Ongoing Monitoring** | The goal of the CDD process is to ensure that LEH understand who their customer is and the purpose for which the customer will use the LEH's services. Where an LEH cannot satisfy itself that it understands a customer, then it must not accept the customer. If there is an existing business relationship, the LEH should not continue it. LEH should also consider filing an suspicious transaction report ("STR") or suspicious activity report ("SAR") or other report types to the FIU as discussed in section 5 of the Guidance.<br>The Standards require three types of KYC processes that must be applied depending on the customer's risk and the nature of the transaction and customer. These are Customer Identification (CID); Customer Due Diligence (CDD); and Enhanced Due Diligence (EDD). Please refer to the table in Section 4.4 on when to use each KYC measure and to the respective paragraphs in the Standards for the detailed requirements.<br>LEH are required to ensure that the documents, data or information obtained under CDD measures are up-to-date and appropriate by reviewing the records, particularly those of high-risk customer categories. Unless otherwise required, LEH should update the KYC information on customers and counterparties on a risk-based schedule, with KYC on higher-risk customers being updated more frequently. When customer's characteristics has changed, LEH should risk-rate the customer again, and, where necessary, conduct EDD. |
| | **Transaction Monitoring** | LEH must continuously monitor all their transactions to ensure that the transactions conducted are consistent with the information they have about the customer, their type of activity and the risks they pose, including, when necessary, the source of funds. All LEH should have a form of transaction monitoring system in place in order to monitor for any suspicious transactions to and from customers; failure to have such a system in place may not only cost an LEH its reputation, but also lead to large fines and other penalties. For more information and details, please consult the CBUAE's *Guidance for Licensed Financial Institutions on Transaction Monitoring Screening and Sanction screening* . |
| | **Sanctions Obligations and Freezing Without Delay** | LEH are required to promptly apply directives issued by the Competent Authorities of the UAE for implementing the decisions issued by the United Nations Security Council under Chapter VII of the Charter of the United Nations and the requirements set by Cabinet Decision 74 of 2020 regarding Targeted Financial Sanctions. For more information and details, please consult the Standards, the Executive Office of the Committee for Goods and Materials Subjected to Import and Export Control's *Guidance on Targeted Financial Sanctions for Financial Institutions and designated non-financial business and professions,* the CBUAE's *Guidance for Licensed Financial Institutions on the Implementation of Targeted Financial Sanctions* as well as the CBUAE's *Guidance for Licensed Financial institutions on Transaction Monitoring Screening and Sanctions screening*.<br>Furthermore, LEH must sign up for the Integrated Enquiries Management System (IEMS) introduced by the FIU to automate and facilitate the execution process of requests for information, implementing decisions of public prosecutions and any other type of ML/FT requests. |
| | **Training** | LEH must provide comprehensive AML/CFT compliance training to all employees, which should be relevant to the LEH's ML/FT risks, business activities and up to date with the latest legal and regulatory obligations and internal controls. It should be tailored to particular lines of business within the LEH, equipping employees with a sound understanding of specialized ML/FT risks they are likely to face and their obligations in relation to those risks, and provided to all new employees within thirty calendar days from the date of joining and regularly thereafter proportionate to their ML/FT risk exposure. |

| | | |
|---|---|---|
| **AML/CFT Program (cont'd)** | **Independent Audit** | Independent auditing must be undertaken regularly to review and assess the effectiveness of the AML/CFT compliance policies, procedures, systems and controls, and their compliance with the LEH's obligations by the LEH's Internal Audit Department. In addition, "agreed-upon procedures" for the review of the AML/CFT Compliance function must be performed by external auditors annually. |
| | **Record-Keeping** | LEH must retain all records, documents, data and statistics for all transactions for a minimum period of five (5) years from the date of completion of the transaction or termination of the business relationship or from the closing date of the account. Records must be maintained in an organized manner so as to permit data analysis and, where relevant, the tracking of financial transactions. |
| | **Managing Employee Risk** | The LEH must implement an appropriate recruitment and Know Your Employee ("KYE") process for hiring employees and confirm the background of applicants prior to placing them in employment. The level of vetting procedures applied should reflect the ML/FT risks to which individual employees are exposed in their assigned roles. |
| **Reporting Obligations** | **Reporting to the CBUAE** | LEH must submit reports to the CBUAE, which may be updated from time to time in terms of the frequency and form of submission and their deadline. For the submission of periodical returns/reports via the online system, the LEH must obtain access to the CBUAE reporting portals, such as its Integrated Regulatory Reporting System ("IRR"), Remittance Reporting System ("RRS") and/or other applicable system. |
| | **Reporting to the FIU** | LEH must file without any delay a STR, SAR or other report types with the FIU using the "goAML" portal when they have reasonable grounds to suspect that a transaction, attempted transaction, or funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime. Please consult the CBUAE's *Guidance for Licensed Financial Institutions on Suspicious Transaction Reporting* for further information. |
| **Prohibition of Tipping Off** | The prohibition on tipping off means that the LEH or its employees must not inform customers or any persons or third parties, either directly or indirectly, that their transactions are subject to monitoring, under investigation or have been reported to the FIU as suspicious transactions. | |