الإمارات العربية المتحدة
وزارة العـــــدل

Lawyers' Guide on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations

Prepared by

Anti-Money Laundering and Combating Terrorism Financing Department

Ministry of Justice

1445 H - 2024 A.D.

INDEX

Purposes of the Guide

This Guide is issued and published by the Ministry of Justice for the Designated Nonfinancial Businesses and Professions (Lawyers) to:

1- Ensure adherence to the Federal Decree Law no. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations, its Implementing Regulation issued by Cabinet Resolution no. (10) of 2019, and its Executive Resolutions;

2- Protect lawyers from the use of their law firms in Money Laundering and Terrorism Financing crimes;

3- identify the core duties and obligations of lawyers in accordance with the Federal Decree Law no. (20) of 2018 and its Implementing Regulations and Executive Resolutions;

4- illustrate the reporting modalities and the mechanism for reporting suspicious transactions or suspicious activity;

5- Promote and protect the credibility and integrity of the financial system of the State; and

6- Explain the methods for identification, assessment and mitigation of Money Laundering and Terrorism Financing risks.

This Guide, and instructions and guidance contained therein, is not intended to create any other new legal obligations but has been prepared to illustrate and clarify the obligations and requirements stipulated in the Federal Decree Law no. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations, and its Implementing Regulation and Executive Resolutions. The content of this Guide is illustrative rather than exhaustive and does not therefore replace

The Federal Decree Law no. (20) of 2018 on Anti-Money Laundering, and its Implementing Regulation and Executive Resolutions.

Money Laundering Concept

A large number of criminal activities aims to make profit for an individual or a group of individuals committing the act. Money Laundering deals with the criminal proceeds with the aim of concealing or disguising their illicit origin. When a criminal activity generates large proceeds, the paramount concern to the perpetrator of these activities is to find a way to control funds and profits, without calling attention to his activities. Criminals do this by disguising the true origin, changing the form of, or transferring money to places where it is less likely to attract attention.

The UAE Law defines Money Laundering as “any financial or banking transaction aiming at concealing or changing the true nature of the funds obtained by illegal means, by passing them through banking and financial system to make them appear as legitimate, and then injecting and investing them into legal activities to disguise their illicit origin”.

Money Laundering Crime is any act committed or attempted with the aim of concealing or disguising the true nature of funds obtained by illegal means and making them appear to have come from a legitimate source.

Article (2) of AML Law no. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations states:

"1- Any person, having the knowledge that the funds are the proceeds of a felony or a misdemeanor, and who willfully commits any of the following acts, shall be considered a perpetrator of the crime of Money Laundering:

a. Transferring or moving proceeds or conducting any transaction with the aim of concealing or disguising their Illegal source

b. Concealing or disguising the true nature, source or location of the proceeds as well as the method involving their disposition, movement, ownership of or rights with respect to said proceeds.

c. Acquiring, possessing or using proceeds upon receipt.

d. Assisting the perpetrator of the predicate offense to escape punishment.

2- The crime of Money Laundering is considered as an independent crime. The punishment of the perpetrator for the Predicate Offence shall not prevent his punishment for the crime of Money Laundering.

3- Proving the illicit source of the proceeds should not constitute a prerequisite to sentencing the perpetrator of the Predicate Offence".

Predicate Offence

AML Law no. (20) of 2018 defines Predicate Offence as "any act constituting a felony or misdemeanor under the applicable laws of the State whether this act is committed inside or outside the State when such act is punishable in both countries".

Predicate Offence, by definition, is a felony or misdemeanor punishable in the State, regardless of whether or not it is committed in the State or in any other country so long as such act is criminalized and punishable in both countries, i.e. the State and the other country where the act is committed.

Money Laundering Phases:

The Money Laundering process most commonly occurs in three key stages:

1- Placement.

2- Concealing and Disguising.

3- Integration.

A simple description of these stages is given below:

1- *Placement:*

Use of illicit funds after their division into small amounts in legal investment projects. Money launderer places the illicit proceeds in official financial and banking institutions in a manner that does not draw attention. Placement takes place through the deposit of the dirty money in banks or financial institutions, foreign currency exchange, the splitting up of funds into small amounts and their deposit in banks, the payment of legal loans using laundered funds or the physical cross-border transportation of cash.

2- *Layering:*

This stage aims to disguise the illicit origin of funds deposited in banks, and keep suspicions away from their illicit source to make their tracing difficult, for example through inter-account transfers or the linkage of funds through a set of accounts in different parts of the world, the transfer of money from an institution to another or within several accounts in the same institution, investment of funds in stock or bonds or life insurance products, replacement of funds with tourism or bank cheques, investment in real estate and other legitimate business, or use of shell companies to hide the ultimate beneficial owner or assets.

3- *Integration:*

This stage aims to inject, legitimize and integrate laundered funds into the national or international economy, in form of direct investments in real estate or scarce goods such as antiquities and valuable items or acquisition of shares in companies or their investment in stock exchange, etc.

Concept of Terrorism Financing and Financing of Illegal Organizations

The Federal Decree Law no. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations defines Financing of Terrorism as "any of the acts mentioned in Articles (29) and (30) of the Federal Law no. (7) of 2014 on Combating Terrorism Offences".

It should also be emphasized that Terrorism Financing Offence is a criminal offence that is not subject to statutes of limitation. Terrorism Financing can be defined as:

1- Providing, collecting, preparing or obtaining Proceeds or facilitating their obtainment by others with intent to use them, while knowing that such proceeds will be used in whole or in part for the commitment of a terrorist offense;

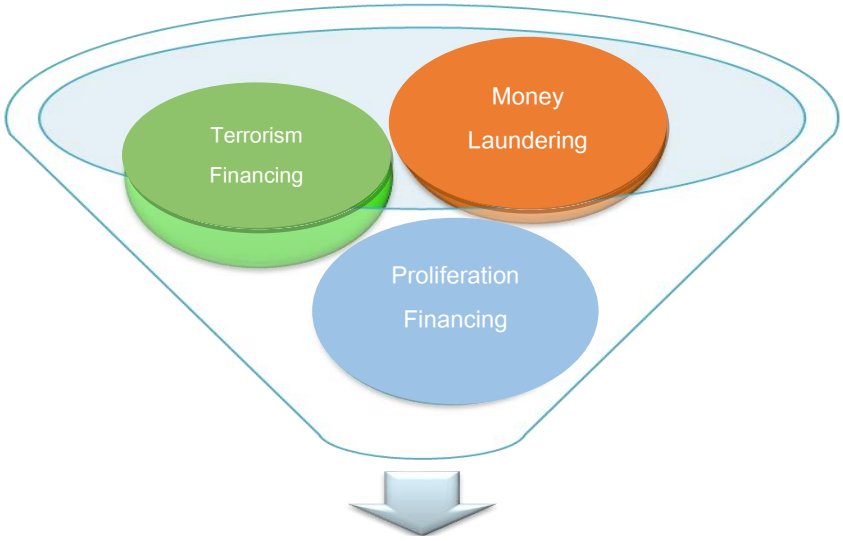
2- Providing, collecting, preparing or obtaining Proceeds or facilitating their obtainment by terrorist organization or a terrorist person, while knowing others with intent to use them, while aware of their true background or purpose;

3- Acquiring, taking, managing, investing, possessing, transferring, moving, depositing, keeping, using or disposing of funds or conducting any banking, financial or commercial transaction while knowing that such funds are, in whole or

in part, the proceeds of a criminal offence or belonging to a terrorist organization or prepared for financing a terrorist organization or terrorist person or a criminal offence.

The Federal Decree Law no. (20) of 2018 defines Illegal Organizations as organizations whose establishment is criminalized or which exercise a criminalized activity. The Decree Law also defines the Financing of Illegal Organizations as any physical or legal action aiming at providing funding to an illegal organization, or any of its activities or its members.

Illicit Financing from International Perspective



Abuse of Financial System for Criminal Purposes

Designated Nonfinancial Businesses and Professions (DNFBP)

Pursuant to the Federal Decree Law no. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations "the Designated Nonfinancial Businesses and Professions (DNFBP)" mean "anyone who conducts one or several of the commercial or professional activities defined in the Implementing Regulation of this Decree Law".

According to the Implementing Regulation issued by Cabinet Resolution no. (10) of 2019, paragraph (3) of Article (3) states that "anyone who is engaged in the following trade or business activities shall be considered a DNFBP:

1- .....

2- .....

3- Lawyers, notaries, and other independent legal professionals and independent accountants, when preparing, conducting or executing financial transactions for their Customers in respect of the following activities:

   (a) Purchase and sale of real estate.

   (b) Management of funds owned by the Customer.

   (c) Management of bank accounts, saving accounts or securities accounts.

   (d) Organizing contributions for the establishment, operation or management of companies.

   (e) Creating, operating or managing legal persons or Legal Arrangements.

   (f) Selling and buying commercial entities.

Relevant Legislation

1- Federal Decree Law no. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations.

2- Cabinet Resolution 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 Organizations.

3- Cabinet Resolution No. (1/3M) of 2019 concerning the Determination of Ministry of Justice as the Supervisory Authority of Lawyers and Notaries in the State.

4- Cabinet Resolution no. (74) of 2020 regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorism Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution.

5- Cabinet Resolution no. (16) of 2021 concerning the Unified List of the Violations and Administrative Fines for Violators of Measures to Combat Money Laundering and Terrorism Financing that are Subject to the Supervision of the Ministry of Justice and the Ministry of Economy.

6- Ministerial Resolution No. (533) of 2019 on the Procedures for Money Laundering and Terrorism Financing for Lawyers and Notaries Public.

7- Ministerial Resolution No. (532) of 2019 on the Establishment of Anti-Money Laundering And Combating Terrorism Financing Department (AML Department).

Lawyers Supervisory Authority

Cabinet Resolution no. (3/1M) of 2019 has been promulgated to establish the institutional framework for supervision of DNFBPs in the UAE. The Cabinet Resolution determined the Ministry as the Supervisory Authority of lawyers and notaries in the UAE.

Ministerial Resolution no. (532) of 2019 has been issued to establish AML Department. Article (4) of this Decision states that "the Department shall be responsible for supervising, monitoring and controlling employers in DNFBPs, including free zones and financial free zones, in accordance with the Ministry's obligations under the Decree Law and its Implementing Regulations".

Anti-Money Laundering And Combating Terrorism Financing Department

Pursuant to the Ministerial Resolution no. (532) of 2019, the competences of AML Department are as follows:

1- Evaluating the risk of commission of the crime in the Sector under Control.

2- Establishing a paper or electronic database for lawyers including all the related data, notably the name, type of activity, date of commencement of practicing the profession and a copy of the license, provided that it is updated continuously.

3- Finding effective and rapid electronic means of communication with lawyers, on both individual and collective levels.

4- Receiving inquiries and providing support and assistance to lawyers through the e-mail of the Department or the hotline designated for this purpose or by any other means.

5- Working on providing periodic training for the staff.

6- Executing and following up the Operational Plan to Combat Money Laundering and the Financing of Terrorism issued by the MOJ.

7- Conducting office and field supervision and inspection on employers in lawyers based on the following:

- The National Risk Evaluation Statement issued by the Committee.
- The crime risks, policies, internal controls and procedures associated with the Sector under Control, as specified in the risk evaluation statement prepared with the knowledge of the Department.

8- Maintaining an up-to-date list of the names and data of the compliance officers with the lawyers and notifying the Unit accordingly.

9- Preparing the Risk Assessment Questionnaire Model, the Suspicious Transaction Report Model and any other relevant models, in coordination with the Financial Information Unit (FIU), and providing it to the lawyers.

10- Organizing awareness-raising programmes and campaigns for lawyers on combatting Crime and giving them the guidance and feedback to enhance their effectiveness in executing of crime combating procedures.

11- Verifying the lawyers' adherence to the implementation of the obligations stipulated in the Decree Law, and the Implementing Regulation.

12- Taking all measures intended to ensure full compliance of lawyers' employees with the implementation of the United Nations Security Council Resolutions (UNSCRs) concerning the Prevention, Suppression and Disruption of Terrorism and its Financing, and the Prevention, Suppression and Disruption of Proliferation of Weapons of Mass Destruction and its Financing, and other relevant resolutions

through field visits and ongoing follow-up, and working to impose appropriate administrative sanctions upon violation or failure to implement the instructions.

13- Informing the Office of the communications, information and data of employers in lawyers regarding the Listed Persons.

14- Preparing reports on the violations committed by lawyers' employees, and presenting them to the Undersecretary.

15- Notifying the lawyers' employees of the decisions imposing the administrative sanctions imposed thereon.

16- Notifying the FIU of the substantiated sentencing decision and the grievance against it.

17- Preparing periodic statistics on measures taken, sanctions imposed and key performance indicators.

18- Receiving applications for grievance against the decisions of listing on local terrorist lists;

19- Receiving the applications of those listed on the local terrorist lists to use a part of the frozen funds and informing the applicant of the decision on the application.

20- Any other competences related to the Supervisory Authorities mentioned in the Decree Law and its Implementing Regulation.

International Organizations

Many international organizations are confronting and combating crimes of Money Laundering, Terrorism Financing and proliferation of weapons of mass destruction. These include:

- The Financial Action Task Force (FATF).

- The International Monetary Fund (IMF).
- The International Organization of Securities Commissions (IOSCO).
- The International Criminal Police Organization (Interpol).
- The Middle East and North Africa Financial Action Task Force (MENAFATF).
- OECD/G20 Inclusive Framework on Base erosion and profit shifting (BEPS).
- The United Nations.

The UAE is a member of, or party to many of these organizations, and their requirements and recommendations are covered by the key aspects of the National Framework for Combating Money Laundering and Financing of Terrorism.

Obligations and Duties of Lawyers

DNFBPs (Lawyers) should implement all the provisions and obligations set out in the Decree Law no. (20) of 2018 and its Implementing Regulation and Executive Resolutions. Such obligations include:

1- Identifying, assessing and understanding the Money Laundering and Terrorism Financing risks;
2- Establishing the appropriate policies and controls to mitigate and curb the risks;
3- Taking customer due diligence measures;
4- Appointing compliance officers;
5- Reporting suspicious transactions;
6- Requirements for modern techniques;
7- Recordkeeping;
8- Training and awareness-raising;
9- Targeted Financial Sanctions.

Identification, Assessment and Understanding of Money Laundering and Terrorism Financing Risks

Lawyers should identify, assess and document Money Laundering risks, provided that risk assessment and the relevant information are updated on periodic basis.

Law firms should also provide risk assessment report and the relevant information to the Supervisory Authorities – Ministry of Justice – upon request. The risk assessment process must be commensurate with the nature and size of the law firm business.

Risk assessment helps lawyers to allocate resources in efficient and effective manner, identify gaps and opportunities for improvement of their policies, controls and procedures relating to combating Money Laundering and Financing of Terrorism, take informed administrative decisions on their risk tolerance and adopt and implement measures and strategies for risk mitigation.

The steps involved in risk assessment process are to identify the inherent risks facing the law firm, the organization or the lawyer and identify how to mitigate such risks effectively through their respective internal policies, controls and procedures.

An important step prior to risk assessment is to be aware that Money Laundering and Terrorism Financing risks are either high or low. In the case of high risks, enhanced measures commensurate with the risks must be implemented to mitigate them. In the case of low risks, the law firm may take palliative measures to manage and mitigate risks. Lawyer may not, however, take palliative measures if there is any suspicion of Money Laundering.

Identification and Assessment of Risks

In identifying and assessing Money Laundering risks, lawyers should identify, assess and understand risks inherent in Money Laundering and terrorism financing in all their activities, and focus on:

- Customer-specific risk factors;
- Risk factors resulting from states or geographical areas where customers conduct their business or which are the source or the final destination of the transaction;
- Risks associated with the nature of products, services, operations and their delivery channels.

In assessing inherent risks, lawyers should make an inventory of customers and products and services delivered to such customers, and countries and areas where customers conduct their business. Risks often occur as combination of risk factors.

Lawyers can formulate risk scenarios for such factors, assess the probability of their occurrence, measure the impact upon occurrence of such scenario. Probability can be evaluated on the basis of number of times a risk can occur in a year, or the impact can be evaluated on the basis of financial and goodwill effects arising if the scenario actually takes place.

On the basis of identified inherent risks, the lawyer can assess whether or not the applicable risk mitigation measures are effective, if there are any residual risks. In the case of residual risks that are beyond the scope of predetermined risks, further controls should be put in place.

Customer-Specific Risks:

Customer risk factors relate to types or categories of customers to whom lawyers deliver services. A specific category of customers or business relationships constitutes risks that should be taken into consideration when assessing the overall level of customer inherent risks.

When identifying specific categories of customers as high-risk by nature, lawyers should consider the results of sectoral or local risk assessment, in addition to the information from official sources including the national risk evaluation, the FATF and the MENAFATF.

The following are some examples of high risks:

1- Commercial relations in unusual circumstances.
2- Customers who do not reside in the State.
3- Legal persons or arrangements which act as asset acquisition vehicles.
4- Companies having nominee shareholders or bearer shares.

Risks Associated with the Nature of Products, Services or Operations and their Delivery Channels

When assessing risks inherent in Money Laundering and Financing of Terrorism related to a service, lawyers should assess their different services that are more likely to be used in Money Laundering and Terrorism Financing. Lawyers should also assess inherent Money Laundering and Terrorism Financing risks from abuse of services by customers, while taking into account a number of factors such as easy retention and transfer of value or its complexity and transparency.

Risks Associated with Countries and Geographical Areas and Delivery Channels

Lawyers can be exposed to geographical Money Laundering and Terrorism Financing risks from local sources and across borders. These risks result from:

1- Areas or locations where the lawyer or the law firm has offices or branches;

2- Areas or locations where customers are domiciled or conduct their business.

With regard to the geographical risks, lawyers and notaries can get information from the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations (NAMLCFTC) on High Risk Jurisdictions and Jurisdictions Under Increased Monitoring.

When assessing risks associated with delivery channels, lawyer should give special attention to such channels which resist or attempt not to disclose their identity. These channels include, without limitation, indirect communication channels, notably in cases where there exist no guarantees such as the electronic identification means – such as internet, telephone or other distance communication technologies or services or the use of third party entities, intermediaries, agents or distributors or the use of third party payment.

Modern Techniques

Lawyer should be familiar with the latest techniques used in Money Laundering and Terrorism Financing, notably when identifying and assessing risks which could arise upon development of new products and new professional practice, including the new service delivery means and the use of new techniques or techniques under development for the new or preexisting products.

Before the launch or use of products, practices or technologies, lawyers and notaries should undertake the appropriate measures to manage and mitigate any specific risks.

Risk Reduction

Law firms should seek to reduce identified risks, taking into account any risks identified at national level and the results of the assessment thereof, through:

1- Establishing internal policies, controls and procedures that are commensurate with the nature and size of the law firm business and approved by the Senior Management, to enable them to manage identified risks and follow up their implementation and enhance them, where appropriate.

2- Taking enhanced due diligence measures to manage high risks once identified. These include:

- To obtain further information and verify the same, including information on customer, beneficial owner or the purpose of business relationship or the reasons for the operation.
- b- to update customer due diligence information on customers and beneficial owners more systematically.
- To take reasonable measures to identify the origin of customer and beneficial owner funds.
- To increase the level and degree of ongoing monitoring of the business relationship and verify operations to identify whether they look normal or suspicious.
- To get the consent of the Senior Management before establishing any business relationship with a customer.

Following the risk assessment and based on the assessment outcomes, law firms should develop and implement internal AML/CFT policies, controls and procedures that identify the appropriate level and type of measures for an efficient and effective management and mitigation of such risks. They should also oversee the implementation of such policies, controls and procedures and enhance them, where necessary.

Establishment of Internal Policies, controls and procedures for Combating Money Laundering and Terrorism Financing

Law firms should develop internal AML/CFT policies, controls and procedures that are commensurate with the risks, nature, size and complexities that may be faced. These should be updated on constant basis.

The above must also be applied to all subsidiaries in which the law firms have majority interest, and must be published and communicated to all employees. Policies and Procedures specifically include:

1- Customer due diligence and business relationship risk management.
2- Suspicious transaction reporting procedures.
3- Appropriate compliance management arrangements for crime prevention, including the appointment of compliance officer.
4- Verification procedures to ensure high competence and suitability standards are in place upon recruitment.
5- Arranging for periodic workshops and programmes in the area of anti-Money Laundering and terrorism financing to build capacities of compliance staff and other concerned employees.

Due Diligence Concept

The Decree Law no. (20) of 2018 and its Implementing Regulation define Customer Due Diligence as the process of identifying or verifying the information of a Client or Beneficial owner, whether a natural or legal person or a legal arrangement, and the nature of its activity and the purpose of the business relationship and the ownership structure and control over it.

Lawyers should undertake customer due diligence measures, before establishing or maintaining any business relationship or conducting any transaction. If such measures cannot be taken, lawyers are prohibited from establishing or maintaining a business relationship or conducting any transaction, and a suspicious transaction report must be communicated to the Financial Information Unit (FIU).

Identifying and assessing Money Laundering risks and taking the reasonable and appropriate customer due diligence measures and ongoing monitoring of customer relations are essential and effective in combating Money Laundering and Terrorism Financing crimes.

In certain cases, lawyers cannot access information or adequately monitor the activities and transactions of their respective customers on constant basis. It is therefore essential to have effective due diligence procedures.

Customer Due Diligence Measures

Lawyers should take customer due diligence measures in the following cases:

1- Start of business relationship.

2- Conduct of occasional transactions equal to, or in excess of AED 55,000 (UAE Dirhams Fifty Five Thousand) for a customer, whether the transactions are individual or multiple and appear to be linked.

3- Conduct of occasional transactions in form of transfers equal to, or in excess of AED 3,500.

4- There is a suspicion of a crime being committed.

5- There are doubts as to the validity or accuracy of the previously obtained customer identification data.

It is prohibited for lawyers to:

1- Deal with fictitious banks in any form, whether by opening bank accounts or accepting funds or deposits from them.

2- Open or hold bank accounts under an assumed, fake or fictitious name, or a numbered bank account.

As stated above, due diligence is a process to be mandatorily observed by lawyers before or during the establishment of business relationship or account opening, or prior to the conduct of any transaction for a customer with whom they have no business relationship. this takes place through several procedures, mainly:

1- To verify the identity of the customer or the ultimate beneficial owner, whether a permanent or occasional, a natural or legal person or a legal arrangement, and that any third party claiming that he acts on behalf of a customer is properly authorized to represent him.

2- To clearly understand the nature and objective of the business relationship with client, provided that it is reasonable and supported by reliable information, and to obtain the relevant information, where required.

3- To understand the nature of business of customers, the ownership structure and control over customer.

4- To exercise enhanced due diligence in respect of high risk customers.

5- To verify the legal status of all customers who have the ultimate ownership or control, or who conduct transactions on behalf of them before the start of the business relationship.

Identity of natural customers and beneficial owners is verified using documents, data or papers obtained from reliable and independent source as follows:

1- Name as it appears in the identity or travel document, accompanied by the certified copy of the valid identity card or the travel document.

2- Nationality.

3- Address and place of birth.

4- Name and address of employer.

5- Obtaining the Senior Management's consent if the customer or the beneficial owner is a politically exposed person.

Identity of clients and beneficial owner who are legal persons and arrangements is verified using documents, data or papers obtained from reliable and independent source as follows:

1- Name, legal form and Memorandum of Association.

2- Address of the head office or the main place of business and, in case of an alien person, the name and address of its legal representative in the State along with the proof thereof.

3- Articles of Association or any other similar documents approved by the relevant entity in the State.

4- Names of relevant persons who hold senior managerial positions in the legal person or arrangement.

Identity of the beneficial owners who are legal persons and legal arrangements is verified using information, data or documents obtained from reliable source as follows:

1- Corporate customers

1. to identify the natural person, whether he works individually or in conjunction with other person who has at least (25%) or more controlling interest in the legal person and, where this is not possible, or if there is any doubt as to the information obtained, to identify him by any other means.

2. if the identity of the controlling natural person cannot be verified in accordance with paragraph (a), or the owner of the controlling interest is not the ultimate beneficial owner, to identify the relevant natural person who holds the senior managerial position, whether he is one person or several persons.

2- Customers from among legal arrangements

To identify the trustor, trustee, or those who hold senior managerial positions, and beneficiaries or categories of beneficiaries, and any natural person who exercises ultimate control over the legal arrangement, and to obtain sufficient information on

the beneficial owner in order to determine his identity when he wants to exercise his rights acquired by law.

Identification of a customer's representative or delegate:

Lawyers should identify any person authorized to act or deal on behalf of a customer, whether such customer is a natural or legal person. When verifying that the person claiming that he acts on behalf of a customer is properly authorized to do so, the following documents are generally deemed as acceptable:

1- A valid power of attorney.

2- An extract of an official record or another official source, proving its ownership or the appointment of the person as duly authorized representative.

3- A court order or another official decision.

Customer due diligence measures must be followed when identifying, and verifying the identity of such persons.

Enhanced Due Diligence

Lawyers should take enhanced due diligence measures to manage and mitigate risks associated with high risk customers and transactions.

High Risk Customers

High risk customers are those who represent a risk, either in person, activity, business relationship, nature or geographical area, such as a customer from a high-risk country or non-resident in a country that does not hold an identity card, or a customer having a

complex structure, performing complex operations or having unclear economic objective, or who conducts cash-intensive operations, or operations with an unknown third party.

Examples of enhanced customer due diligence measures are:

1- To obtain further information and verify the same, including information on customer, beneficial owner or the purpose of business relationship or the reasons for the transaction.

2- To update due diligence information on customers and beneficial owners more systematically.

3- To take reasonable measures to identify the origin of customer and beneficial owner funds.

4- To increase the level and degree of ongoing monitoring of the business relationship and verify operations to identify whether they look normal or suspicious.

5- To get the approval of the senior management before establishing any business relationship with a customer.

6- When taking such procedures, lawyers should pay particular attention to the reasonableness of the information obtained, and should evaluate it for possible inconsistencies or conflicts and for unusual or suspicious circumstances.

Politically Exposed Persons (PEPs)

Due to their potential ability to influence government policies, determine the outcome of public funding or procurement decisions, or obtain access to public funds, politically exposed persons (PEPs) are classified as high-risk individuals from an AML/CFT perspective. The Decree Law no. (20) of 2018 defines PEPs as:

“Natural persons who are or have been entrusted with prominent public functions in the State 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. The definition also includes:

1- Direct family members (of the PEP, who are spouses, children, spouses of children, parents)
2- Associates known to be close to the PEP, such as individuals having individual or joint ownership rights in a legal person or arrangement established in favour of the PEP or any other close business relationship with the PEP”.

Lawyers should put in place appropriate policies and procedures to manage risks and identify whether a customer or a beneficial owner is a PPE. In addition to the standard due diligence procedures, lawyers are also required to:

1- Take reasonable measures to establish the source of funds of customers and beneficial owners classified or identified as PEPs.
2- Evaluate the legitimacy of the source of funds and the origin of wealth, including making reasonable investigations into the professional and financial background of PPEs.
3- Obtain the senior management’s consent before establishing a new business relationship with a PPE, or before continuing an existing one and increase the ongoing monitoring of such relationship.

In the case of PPEs and individuals who were previously entrusted with prominent positions at international organizations, lawyers should implement the above measures when classifying the business relationship with such persons as high risk relationship.

Notably, the potential risk factors consist in the level of (unofficial) influence a person is able to exercise, the seniority of position held by the PPE, or whether his former or current position is in any way linked, for example, through the appointment of a successor to the PPE, or unofficially if the PPE still deals with the same substantive matters).

High Risk Countries

Lawyers should apply enhanced due diligence measures that are commensurate with the risks associated with business relationships or operations with a natural or legal person from any high risk country.

Law firms should apply measures established by the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organizations (NAMLCFTC).

High Risk Countries are countries identified as those with key strategic weak measures to combat Money Laundering and Terrorism Financing and financing of proliferation of weapons, and classified within the list of high risk jurisdictions at international level according to the list issued by The Financial Action Task Force (FATF) or as specified by the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organizations (NAMLCFTC).

List of High Risk Jurisdictions can be found on the website of the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organizations (NAMLCFTC) at https://namlcftc.gov.ae/ar.

For further information, relevant guidelines issued by FATF can be found on the website: https://www.fatf-gafi.org.

Simplified Due Diligence

In certain circumstances and in case there is no suspicion of Money Laundering or Terrorism Financing crime, lawyers may take simplified due diligence measures on customers identified as low risk ones through a sufficient risk analysis. Simplified due diligence process is generally a more lenient application of due diligence process and needs to be commensurate with the identified low risks. Simplified due diligence procedures include, without limitation:

a- Verifying the identity of the customer and the beneficial owner after establishing the business relationship.

b- Updating the customer details at intervals.

c- Reducing the ongoing monitoring and verification of operations.

d- Inferring the purpose and nature of the business relationship from the type of transactions or the established business relationship, without need for gathering information or undertaking specific procedures.

Ongoing monitoring during Business Relationship

Lawyers should monitor the customer activity on ongoing basis and audit and supervise the operations carried out throughout the business relationship to ensure their

consistency with information being obtained, the kinds of activity and the customer-specific risk profiles. They should also investigate into the source of funds, when and where necessary.

Lawyers should use a risk-based approach to identify policies, controls and procedures applied by them in monitoring customer transactions and activities, and the extent of monitoring of specific customers or specific categories of customers.

The review and timely update of simplified due diligence information are crucial for an effective mitigation of Money Laundering and Terrorism Financing risks.

Lawyers should also keep customer and beneficial owner documentation, data and information up-to-date and adequate through the review of documents, notably high risk customer records. Information on high risk customers should be updated on constant and more frequent basis. In the case of low risk customers and if there is no suspicion of Money Laundering or Terrorism Financing, simplified due diligence information can be updated less frequently.

When suspecting that a crime has been committed, lawyers may not undertake customer due diligence measures if they have reasonable grounds to believe that such due diligence measures would attract the attention of the customer.

In this case, lawyers should submit a suspicious transaction report to FIU along with the reasons for not applying such measures.

Exemption from Identifying the Shareholder, Partner or Beneficial Owner

Lawyers are exempted from identifying and verifying the identity of any shareholder, partner, or the Beneficial Owner, if such information is obtainable from reliable sources where the customer or the owner holding the controlling interest are either a company listed on a regulated stock exchange subject to financial control and disclosure requirements or a subsidiary whose majority shares or stocks are held by a holding company.

What to do if Due Diligence Measures cannot be applied?

Law firms are prohibited from establishing or continuing any business relationship or conducting any transaction if customer due diligence measures cannot be taken, and should communicate a suspicious transaction report to FIU.

Third Party Reliance

Lawyers may rely on a third party to undertake customer due diligence measures in specific circumstances and pursuant to the controls set by Article (19) of the Implementing Regulation of Decree Law no. (20) of 2018.

When relying on a third party, lawyers should immediately obtain from such third party the necessary identification details and other necessary information collected through due diligence measures, and ensure that copies of the necessary documentation for such measures are obtained without delay upon request. Lawyers should also ensure that such third party is regulated and under control and observes customer due

diligence measures and keep records in line with the requirements of the Decree Law no. (20) of 2018 and its Implementing Regulation.

Lawyers should ultimately remain liable for the accuracy of such measures and the outcomes of the customer due diligence process.

Engagement of Compliance Officer

The Law Firm should engage a compliance officer with the appropriate competence and expertise to carry out the following tasks and functions:

1- Detect transactions related to the crime.

2- Review the records and receive, examine and consider information on suspicious transactions and decide either to notify FIU or close the same along with the reasons, in complete confidentiality.

3- Review the internal regulations and procedures relevant to the combating of Money Laundering and Financing of Terrorism and financing of illegal organizations, and check their consistency and conformity with the provisions of Decree Law and its Implementing Regulation.

4- Evaluate the compliance of his law firm with the regulations and procedures relevant to the combating of Money Laundering and Financing of Terrorism and financing of illegal organizations, and suggest what need to be done for their update and development.

5- Prepare bi-annual reports and present them to the Senior Management, with copy to the Anti-Money Laundering and Combating Terrorism Financing Department at the Ministry of Justice, including comments and decisions of the Senior Management.

6- Put in place, implement and document constant programs and training plans for law firm personnel in respect of the Money Laundering, Financing of Terrorism and financing of illegal organizations and how to combat them.

7- Cooperate with the Ministry of Justice, the FIU at the Central Bank and other competent authorities in the State, provide information and data, and enable their personnel access to records and documents necessary for the discharge of their duties.

8- Verify the suspicious transactions and report the same to the FIU and provide the required information and cooperate with the Ministry of Justice and the other competent authorities in the State.

Compliance Officer shall meet the following criteria:

1- He must be above the age of 21 years.

2- He must have a degree from any university or high institute accredited in the State, or the equivalent thereof.

3- He must have the appropriate competence and experience.

4- He must be of good character and conduct, and must not be convicted of a felony or an offence involving honesty, honor or subjected to a disciplinary sanction for any of such offences.

In any event, it is mandatory to obtain the consent of the AML Department before the appointment of the Compliance Officer.

Suspicious Transaction Reports

in the case of suspicion or reasonable grounds to suspect a Money Laundering crime, lawyers should promptly communicate a suspicious transaction report to FIU through FIU's goAML.

Suspicious Transactions are transactions related to funds for which there are reasonable grounds to believe that they are earned from any misdemeanor or felony or related to the Financing of Terrorism or of illegal organizations, whether committed or attempted.

Notwithstanding their value or timing, these transactions are either:

- Proceeds of any offence (whether felony or misdemeanor, and whether committed in the State or other State in which it constitutes an offence).
- Related to crimes of Money Laundering, Financing of Terrorism or financing of illegal organizations.
- Intended for use in activities connected with such crimes.

Lawyers and their personnel should not, directly or indirectly, disclose to customers or any other person that they reported such client to FIU or are about to report:

1. That a report has been prepared or is intended to be prepared.
2. Information or data in the report.
3. That there is an ongoing investigation into the transaction.

Lawyer's attempt to persuade the customer not to act against the law is not considered as disclosure.

Communication of Suspicious Transaction Report does not require an evidence that a predicate crime has actually been committed or that there is an illicit source of proceeds. Only reasonable grounds for suspicion are required and can be deduced from certain information such as:

- Suspicious transactions or indicators thereof.
- kinds of treatment or behavior.
- Customer due diligence information.

Confidentiality:

Lawyers should keep confidential information being reported and make reasonable efforts to procure the protection of such information or data from any unauthorized access. Adequate policies, controls and procedures need also to be developed by law firms to guarantee the confidentiality of information and data relating to suspicious transaction reports and their protection, including a statement of suspicious transaction reporting procedures.

Law firms should set indicators by which they can identify any suspicious offence for suspicious transaction reporting purposes. They should also update the same on constant basis depending on the development and diversity of methods of committing such offences, and should abide by the instructions of the supervisory authorities or the FIU in this respect.

in the case of suspicion or reasonable grounds to suspect that a transaction or attempted transaction or money represents, in whole or in part, proceeds, or is connected with a crime, or will be used in its commission notwithstanding its value, the law firms should, without invoking bank secrecy, professional or contractual secrecy:

1- Communicate the suspicious transaction report to the FIU, without delay, through goAML or any other means approved by the FIU.
2- Provide any further information as may be required by the FIU.

Lawyers are exempted from reporting obligations if information relating to such transactions is obtained on the occasion of the evaluation of the legal status of the client or to defend or represent him in court, arbitration or mediation proceedings or the provision of legal opinion in a matter related to judicial proceedings, including an advice on initiating or avoiding such proceedings, whether such information has been obtained prior to, during or following the judicial procedures or in other circumstances where they are subject to professional secrecy.

The lawyer or his personnel should not have any administrative, civil or criminal liability to the reported person in case of good faith reporting or submission of any information to the FIU.

Responsibility to Report

Compliance Officer in the law firm has the duty to report any suspicious transactions to the FIU through goAML for suspicious transactions reporting.

A lawyer or a law firm employee has also the duty to report any suspicious transactions to the Compliance Officer.

All law firms should therefore establish the appropriate policies, procedures, controls and training courses on the internal reporting procedures (reporting from directors and personnel) of the suspicious transactions (including the provision of the necessary

records and information) to Compliance Officer for combating Money Laundering and Financing of Terrorism for further analysis and making the necessary decision.

Timing of Reporting

Pursuant to the Implementing Regulation, suspicious transactions should be reported "without delay".

In other words,
Employees in law firms should observe the internal reporting of suspicious transactions to the compliance officer in the case of suspicion or reasonable grounds to suspect a crime.

External reporting of suspicious transactions by the compliance officer to the FIU shall be made at the moment when he determines that the transaction gives rise to suspicion and must be reported.

Financial Information Unit (FIU)

Financial Information Unit at the Central Bank of the United Arab Emirates (CBUAE) is the official financial information entity.

The FIU works independently under a legal and regulatory delegation as national central authority and is entrusted, inter alia, with:

1- Establishing a database or special register for information it may have, and protecting the same by setting up rules governing information security and confidentiality.

2- Providing training courses and programs for its staff and any other entity, whether inside the UAE or abroad.

3- Preparing studies, researches and statistics related to the crime, and following up any studies, researches or statistics made at national or international scale in this respect.

4- Receiving reports from financial institutions and DNFBPs, according to the relevant forms, and considering, analyzing and archiving the same in its database.

5- Requesting the provision of any other information or documents related to suspicious transaction reports, and other information it may deem necessary from the entities subject to supervision and competent authorities, including information on declaration system.

6- Forwarding information on suspicious transaction reports to the national law-enforcement agencies, the judicial authorities and public prosecutions.

7- Sharing information with its counterparts in other states in accordance with the international conventions to which the State is a party or any MOUs made by the FIU with its counterparts to regulate the mutual cooperation, or on the basis of reciprocity.

Handling Transactions after Submission of Suspicious Transaction Report

Once the Compliance Officer submits a suspicious transaction report to FIU, the law firm should follow the instructions that may be issued by the FIU. In addition, the customer should immediately be classified as high risk customer and the appropriate

enhanced due diligence measures and the ongoing monitoring procedures should be undertaken until instructions and directions are received from FIU.

Instructions issued by FIU to law firms submitting a suspicious transaction report include, without limitation:

1- Instructions to reject the transaction.
2- Instructions to allow the completion of the transaction (such as in cases of controlled delivery of funds in order to allow them to be traced by the Competent Authorities).
3- Instructions to freeze or attach the funds or other assets of the customer.
4- Instructions to end the business relationship.
5- Instructions to maintain the business relationship and regularly monitor and report the activities to FIU and/or the other Competent Authorities.
6- Requests for additional information on the reported transaction and other transactions related to the customer or connected with the business relationship in general.

Confidentiality should also be guaranteed and the law firm must adhere to all instructions and requests of FIU.

Requirements for New Techniques

Lawyers should stay abreast of new techniques used in Money Laundering, in particular:

1- The identification and assessment of risks which could arise upon development of new products and new professional practice, including the new service delivery

means and the use of new techniques or techniques under development for each of the new or preexisting products.

2- The assessment of risks before the launch or use of products, practice, techniques, and the implementation of the appropriate measures to manage and mitigate such risks.

Recordkeeping

Law firms should maintain transaction records containing:

1- All documents, papers and data with regard to all local or international financial transactions and commercial and financial dealings.

2- All documents obtained through customer due diligence measures and ongoing monitoring, the accounts and commercial correspondence files and copies of personal identity documents, including the suspicious transaction reports and the outcomes of any analysis conducted.

3- Records and papers and documents contained therein must be in order in order to allow data analysis and tracing of financial operations.

Recordkeeping Period

DNFBP should retain the records for a minimum period of (5) five years in the following cases:

- From the date of completion of the transaction.
- The end of the business relationship with the client.
- End of business relationship.
- From the date of closure of accounts for customers.
- After completion of an occasional transaction.

- From the date of end of inspection by the Department
- From the date on which investigation is completed.
- From the date on which a final judgment is rendered by the competent judicial authorities.

All the above, as appropriate.

Making Information & Records available

Law firms should promptly make all customer information related to customer due diligence and ongoing monitoring and the outcomes of their analysis, and records, files, documents, correspondence and forms, available to the relevant entities upon request.

Training and Awareness-Raising

In order to assess risks associated with Money Laundering and Terrorism Financing crimes and for effective mitigation measures, law firms should procure that all their employees have a clear understanding of Money Laundering and Terrorism Financing risks and appropriate procedures and decisions are in place when the firm is exposed to any attempted use or in case of any suspicion on a customer or suspicious transactions.

In addition, given the ever-evolving nature of Money Laundering and Terrorism Financing crimes, law firms should procure that their employees are constantly familiar with the latest developments in respect of new risks and internal and external risks associated with Money Laundering and Terrorism Financing crimes, and should procure that training records are kept and made available to the Ministry's inspectors upon request.

In order to be effective, the training programme should not be limited to the clarification of AML/CFT laws and regulations but needs to include internal policies and procedures used for the mitigation and assessment of risks and the understanding of responsibilities and duties of lawyers pursuant to the relevant legislation in force.

It should be noted that AML Department at the Ministry puts in place an annual training plan and organizes a number of training workshops and courses in AML-CFT field, in cooperation with specialized entities. AML Department invites all lawyers and personnel of law firms to attend such training courses and workshops and improve awareness in general, bearing in mind that all such workshops and courses are free of charge.

Targeted Financial Sanctions

The term Targeted Sanctions includes sanctions that are imposed on specific individuals, entities, groups or organizations.

The term targeted financial sanctions includes both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of individuals, entities, groups, or organization subject to sanctions.

What is the purpose of Targeted Financial Sanctions?

The purpose of targeted financial sanctions is to deny certain individuals, groups, organizations, and entities the means to support terrorism or finance the proliferation of weapons of mass destruction. To this end, it seeks to ensure that no funds, financial assets, or economic resources of any kind are available to listed actors for so long as they remain subject to the restrictive measures.

Law firms should:

1- Register in the Executive Office of Committee for Goods Subject to Import and Export Control for automatic email notifications.

Registration aims to help law firms to receive an up-to-date information in due time about the listing of persons on local list and UN Security Council List or their removal from such list.

2- Verify: conduct regular verifications of the following databases to identify any potential conformities with the names listed on UN Security Council List or local lists, including:

1. Customer databases.
2. Names of parties to any transactions.
3. Potential customers.
4. Beneficial owners.
5. Names of individuals or entities directly or indirectly related to them.
6. Customer before the conduct of any transaction or the establishment of any serious business relationship with any individual.

3- Apply the freezing measures: without delay (within 24 hours), and without prior notice to the listed individual or entity, once a match is detected during the verification process.

4- Notify the Executive Office of the Committee for Goods Subject to Import and Export Control within (1) one business day of the application of freezing measures and all additional information.

5- Put in place and implement:

1. Internal controls and procedures to ensure the compliance with obligations arising out of this decision.

2. Policies and procedures that prohibit the employees from directly or indirectly informing the customer or any third party that freezing or any other measures are being applied in accordance with the provisions of this decision.

   Through internal controls, policies and procedures, a law firm may identify the process and practices to implement these measures, taking into account the specificities of its business and customers.

6- Cooperate with the Executive Office of the Committee for Goods Subject to Import and Export Control in the verification of accuracy of information provided.

National and International Sanctions List

The Cabinet Resolution No. (74) of 2020 regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorism Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolutions, includes two kinds of sanctions lists related to individuals and entities:

1- UAE List of Terrorists issued by the Cabinet

   This List includes the names of individuals, entities and organizations which committed, planned for, proliferated or financed a terrorist activity.

2- UN Security Council Sanctions List

   This List includes the names of individuals, entities and organizations which the United Nations consider that they conduct activities against development and peace.

Such names are mostly involved in terrorist acts, genocides and violation of international law.

It should be noted that UN Security Council Sanctions List and UAE List of Terrorists can be found online through the website of the Committee for Goods Subject to Import and Export Control: https://www.uaeiec.gov.ae/ar-ae/.

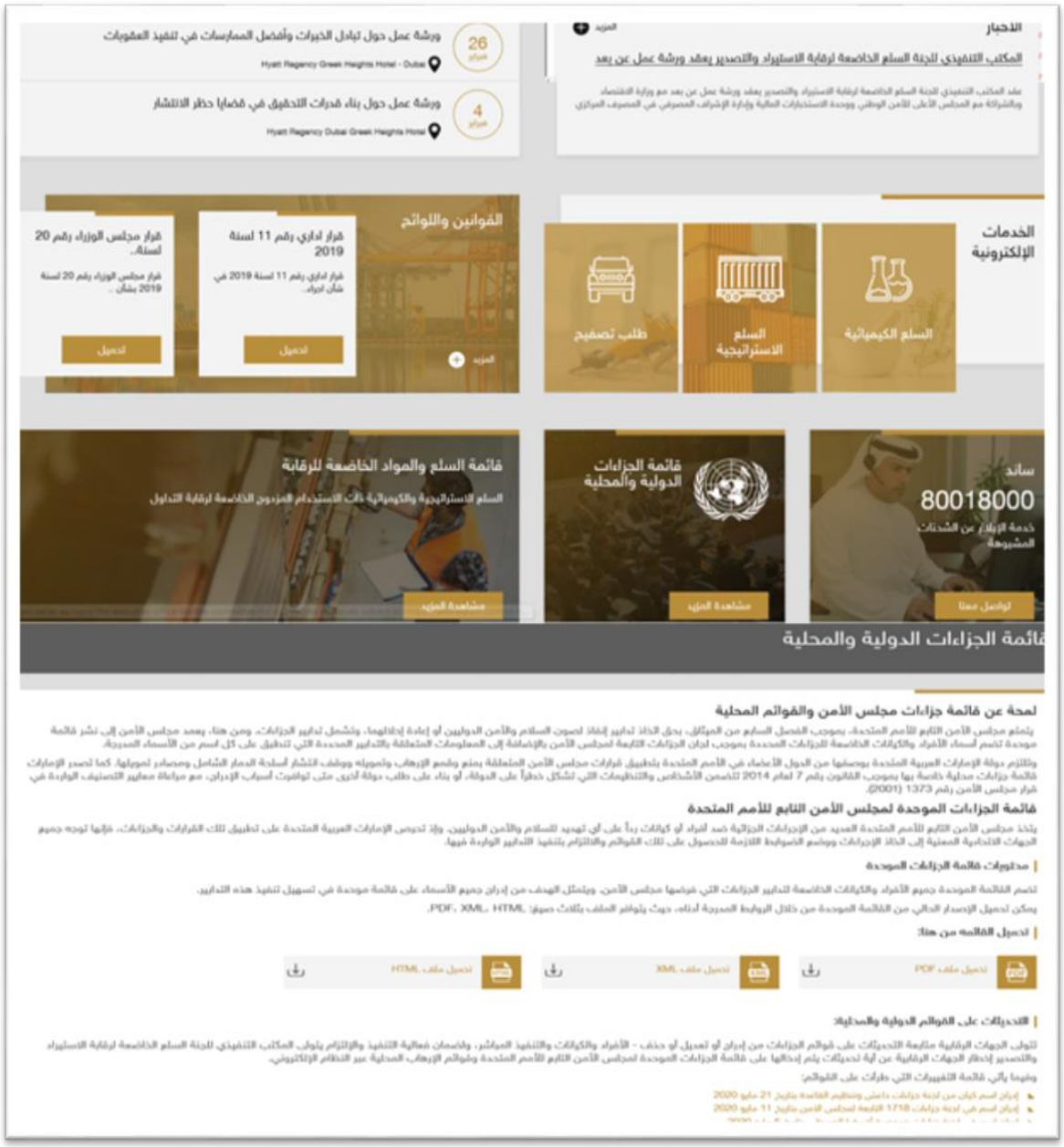
It must also be noted that such lists are subject to regular update, whether by deletion, amendment or addition of new names. Lawyers are therefore required to review the lists regularly or upon reporting of any amendment or updating such lists.

Subscription to email notifications can be made through the website of the Executive Office to ensure that the latest updates on the lists are obtained.

Lawyers have the obligation to conduct a periodic inspection and audit of existing and potential customer database and verify if any names are compatible with any listed person. customer database is verified in case new names are listed without delay.

Expression “without delay” means within hours of any listing by the UN Security Council or the UAE Cabinet.

Online Platform of the Executive Office



The online platform developed by the Executive Office of the Committee for Goods Subject to Import and Export Control for the publication of Lists of Sanctions/Penalties issued by the UN Security Council and the UAE Cabinet has many advantages, namely:

1. All supervisory authorities are registered in the online platform to receive any update on the UN Security Council List or the National Terrorist List immediately, and any feedback in case any information on the listed persons is available.
2. The platform enables all entities to get the latest update on the Sanctions List at any time.
3. The website includes an indication of procedures for filing grievance by the listed person residing in the State.
4. Any user can subscribe to receive updates on the lists.

You can contact the Executive Office at sanctions@uaeiec.gov.ae.

Administrative Sanctions

The Supervisory Authority may impose administrative sanctions in case the law firm, or an employee thereof, violates any provisions of the Decree Law or its Implementing Regulation, in the following manner:

1. AML Department shall notify the offender of the violation attributed to him.
2. The offender must submit a response with supporting documents within (5) working days from the date of his notification.
3. AML Department sends a report to the Undersecretary after the expiry of the aforementioned period, stating and identifying the violation, the reply of the offender thereto , if any, and the Department's recommendation on the action to be taken against the offender.

Once the violation is established, a reasoned decision shall be issued by the Undersecretary to impose any of the following administrative sanctions on the offender:

a. Warning
b. Administrative fine ranging between AED 50,000 (UAE Dirhams Fifty Thousand) and AED 5,000,000 (UAE Dirhams Five Million) per violation.
c. Preventing the offender from the exercise of profession in the relevant sector for the term stipulated in the decision.
d. Limiting the powers of directors whose liability for the violation is established. The decision may include an appointment of a temporary controller.
e. Suspending the director whose liability for the violation is established, for the period specified by the decision or requiring his change, if permitted.
f. Suspending or limiting the practice of the profession for the period set out in the decision.
g. Cancellation of the license.

Except for paragraph (g), the Undersecretary may, when applying the administrative sanctions, require regular reports to be submitted on the measures taken to rectify the violation.

AML Department shall notify the offending lawyer of the sanction decision within (15) fifteen days from the date of its issuance. The Department may publish any administrative sanctions imposed in the various means of publication.

Grievance against the Administrative Sanctions

Offender may file a grievance to the Minister of Justice against the decision imposing the administrative sanction within (15) fifteen days from the date on which he is notified or becomes aware thereof. The Minister's decision on the grievance shall be final. Non-response to the grievance within (30) thirty days from its submission shall be considered as dismissal of the grievance.

No appeal against the decision imposing administrative sanction may be accepted before making a grievance against it, rejecting it or the lapse of the time for response thereto.

Penalties

The Federal Decree Law no. 20 of 2018 provides for a number of penalties in connection with crimes of Money Laundering and Financing of Terrorism. Lawyers must be familiar with, and fully aware of the penalties in case of non-compliance with the duties and obligations prescribed by law.

Where To Get Assistance Or Further Information

Anti-Money Laundering and Combatting Terrorism Financing is a very hard, complex and ever-changing process. DNFBPs must procure that their Compliance Officers and personnel are always familiar with any developments in this area. To this end, some sources of further information are suggested below:

National competent authorities such as the Ministry of Justice, Financial Information Unit (FIU) of CBUAE and NAMLCFTC.

Websites of the Financial Action Task Force (FATF), the Middle East and North Africa Financial Action Task Force (MENAFATF) and other similar regional offices.

The website of United Nations Office on Drugs and Crime.

You can contact Anti-Money Laundering and Combating Terrorism Financing Department at the Ministry of Justice at amlctf@moj.gov.ae. You can also visit the website of the Ministry on https://www.moj.gov.ae, which contain all AML/CTF legislation and decisions, guidebooks and important links that help lawyers access information as quickly as possible.

*** END ***

Prepared by

Chancellor Abdullah Ahmed Al Rashid

Head, Anti-Money Laundering and Combating Terrorism Financing Department

9-4-2024