ALYIANT
Consultancy Limited

ALYIANT2YOU : Regulatory Brief

AML Legislation Compliance - UAE

Introduction

Robust legislation and measures have been implemented by the United Arab Emirates ("**UAE**") with respect to Anti-Money Laundering, Combating the Financing of Terrorism and Financing of Illegal Organisations, and Sanctions (referred to herein for ease of reference as "**AML**"). Legislative measures are primarily contained in and implemented pursuant to: (i) Federal Law No.20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations ("**Federal Law No. 20 of 2018**"); (ii) Cabinet Decision No.10 of 2019 concerning the Implementing Regulations of Federal Law No.20 of 2018 ("**Cabinet Decision No.10 of 2019**"); (iii) Cabinet Decision No.74 of 2020 regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combatting of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolutions ("**Cabinet Decision No.74 of 2020**"); and (iv) Federal Law No.7 of 2014 on Combating Terrorism Offences (**"Federal Law No.7 of 2014"**). The above and related legislation are collectively referred to herein as the "**Federal AML Legislation**".

The Federal AML Legislation is applicable across the UAE in its entirety, including in the UAE's two financial free zones, namely: the Dubai International Financial Centre ("**DIFC**") and the Abu Dhabi Global Market ("**ADGM**"). Cabinet Resolution No. 28 of 2007 (on the Implementing Regulations of Federal Law No.8 of 2004 Concerning Financial Free Zones) provides that: (i) financial free zones (e.g. the DIFC and ADGM) and all operations conducted therein shall be subject to the provisions of the federal laws applicable in the UAE concerning the criminalization of money laundering and anti-terrorism finance; and (ii) the financial free zones and financial activities shall also be subject to all federal laws, with the exception of civil and commercial federal laws. The DIFC and the ADGM have also put in place respective rules for AML compliance which apply alongside the Federal AML Legislation.

We examine the Federal AML Legislation, and the AML rules implemented in the DIFC. AML matters in the DIFC are governed by two separate and complimentary frameworks of: (a) the Federal AML Legislation and (b) DIFC Regulatory Law 2004 (**"Regulatory Law"**) and the Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module of the Dubai Financial Services Authority Rulebook (referred to herein as the "**AML Module**") in respect of a "Relevant Person". This paper focuses on several aspects of the obligations of "Financial Institutions" and "DNFBPs" under the Federal AML Legislation, and the obligations of a "Relevant Person" under the AML Module.

The coverage in this paper of the Federal AML Legislation and the AML Module is non-exhaustive and general in nature. Accordingly, the provisions of the Federal AML Legislation and AML Module (including the applicable definitions of terms and references set forth therein) should be reviewed in their totality for a detailed understanding of the applicable provisions thereof.

Implementation of AML Legislation in the UAE

The UAE continues to ramp up the fight against financial and related crime through various progressive processes, including by way of the Federal AML Legislation, the AML Module (in connection with the DIFC), and the UAE's continuing commitment in connection with and effective implementation of the FATF Recommendations. The Financial Action Task Force ("**FATF**") is a major catalyst for the international approach to AML compliance, and is the global money laundering and terrorist financing watchdog established by the G-7 Summit that was held in Paris in 1989. The FATF sets international standards that aim to prevent the illegal activities of money laundering, terrorist financing and related matters. The UAE is a member of the Co-operation Council for the Arab States of the Gulf ("**GCC**"). The GCC is a member of the FATF. As an FATF member, the GCC is committed to implementing the anti-money laundering, counter-terrorist financing and related measures agreed to by the FATF members. The FATF developed the "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation" (the "**FATF Recommendations**"), which were adopted by the FATF Plenary in 2012. There are 40 FATF Recommendations and to achieve global implementation of the 40 FATF Recommendations, several FATF-Style Regional Bodies (FSRBs) have been established in addition to the 39 FATF members. The Middle East and North Africa Financial Action Task Force ("**MENAFATF**") is one the FSRBs. The UAE is a member of MENAFATF and the UAE's commitment to

fighting financial and related crime has culminated in the Federal AML Legislation and in the case of the DIFC, the AML Module. The Federal AML Legislation and in the case of the DIFC, the AML Module, are in alignment with the FATF Recommendations.

Federal Law No. 20 of 2018

Federal Law No.20 of 2018 repeals the earlier Federal Law No.4 of 2002 on the criminalization of money laundering and combatting of the financing of terrorism. Federal Law No.20 of 2018 makes provision for, amongst other matters: the crime of Money Laundering; the crime of Financing of Terrorism; the crime of Financing Illegal Organisations; the establishment in the UAE of the Financial Intelligence Unit (which we refer to herein as the "**UAE FIU**"); the establishment in the UAE of the "National Committee for Combatting Money Laundering and the Financing of Terrorism and Illegal Organisations" (which we refer to herein as the "**UAE NAMLCFTC**"); the responsibilities of "Supervisory Authorities"; the obligations of **"Financial Institutions"** and Designated Non-financial Businesses and Professions ("**DNFBPs**"); and penalties and consequences for violation of Federal Law No. 20 of 2018.

Federal Law No. 20 of 2018 definition of Money Laundering

"Money Laundering" is defined as any of the acts in Article 2(1) of Federal Law No.20 of 2018, which in essence states that any person having the knowledge that funds are the proceeds of a felony or a misdemeanour and who wilfully 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 the said proceeds; (c) acquiring, possessing or using proceeds upon receipt; (d) assisting the perpetrator of a predicate offence to escape punishment. Article 2(1) is stated to be without prejudice to the provisions of Federal Law No.7 of 2014 and Federal Law No. 3 of 1987 with respect to the UAE Penal Code and its amendments ("**Federal Law No.3 of 1987**").

Federal Law No. 20 of 2018 definition of "Financing of Terrorism"

"Financing of Terrorism" is defined with reference to Articles 29 and 30 of Federal Law No.7 of 2014. Articles 29 and 30 of Federal Law No.7 of 2014 set forth in detail "Terrorism Financing Offences". Article 3(1) of Federal Law No.20 of 2018 in essence provides that whoever intentionally commits any of the following is guilty of the crime of financing terrorism: (a) any of the acts specified in Article 2(1) of Federal Law No.2 of 2018 (i.e. see above with respect to the crime of "Money Laundering"), if he is aware that the proceeds are wholly or partly owned by a terrorist organisation or terrorist person or intended to finance a terrorist organisation, a terrorist person or a terrorist crime, even if it is without the intention to conceal or disguise their illicit origin; (b) providing, collecting, preparing or obtaining proceeds or facilitating their obtainment by others with intent to use them, or while knowing that such Proceeds will be used in whole or in part for commitment of a terrorist offence, or if he has committed such acts on behalf of a terrorist organisation or a terrorist person while aware of the true background or purpose. Article 3(1) is without prejudice to the provisions of Federal Law No.7 of 2014 and Federal Law No.3 of 1987.

Federal Law No. 20 of 2018 definition of "Financing of Illegal Organisations"

"Illegal Organisations" are defined by Federal Law No.20 of 2018 as organisations whose establishment is criminalised or which exercise a criminalised activity. Cabinet Resolution No.10 of 2019 contains a similar definition. "Financing of Illegal Organisations" is defined in Federal Law No.20 of 2018 and in Cabinet Decision No.10 of 2019 as: any physical or legal action aiming at providing funding to an illegal organisation, or any of its activities or members. Article 3(2) of Federal Law No.20 of 2018 in essence provides that whoever intentionally commits any of the following is guilty of financing illegal organisations crime: (a) any of the acts specified in Article 2(1) of Federal Law No.20 of 2018 (i.e. see above with respect to the crime of Money Laundering), if he is aware that the proceeds are wholly or partly owned by an illegal organisation or by any person belonging to an illegal organisation or intended to finance such illegal organisations or any person belonging to it, even if without the intention to conceal or disguise their illicit origin; (b) providing, collecting, preparing, obtaining proceeds or facilitating their obtainment by others with intent to use such proceeds, or while knowing that such proceeds will be used in whole or in part for the benefit of an illegal organisation or of any of its members, with knowledge of its true identity or purpose. Article 3(2) is stated to be without prejudice to the provisions of Federal Law No.7 of 2014 and Federal Law No.3 of 1987.

ALYIANT2YOU : Regulatory Brief

Federal Law No.20 of 2018 - Definition of "Crime"

Federal Law No.18 of 2020 and its implementing regulation Cabinet Decision No.10 of 2019 in several provisions refer to the term "Crime"/"crime", which is defined in Federal Law No.18 of 2020 and in Cabinet Decision No.10 of 2019 in essence as: "Money Laundering crime and related Predicate Offences, or Financing of Terrorism or Illegal Organisations" (note: see also the discussion above on the crimes of "Money Laundering", "Financing of Terrorism" and "Financing Illegal Organisations"). A "Predicate Offence" is also similarly defined in Federal Law No.20 of 2018 and Cabinet Decision No.10 of 2019 in essence as: any act constituting an offence or misdemeanour under the applicable laws of the UAE whether such act is committed inside or outside the UAE when such act is punishable in both countries. The definition of the term "Crime"/ "crime" is kept in mind in the discussion below on Federal Law No.18 of 2020 and Cabinet Decision No.10 of 2019 where it is referred to.

Obligations of Financial Institutions and DNFBPs under Federal Law No.20 of 2018

Financial Institutions and DNFBPs have specific obligations under Federal Law No.20 of 2018. "Financial Institutions" are defined by reference to Cabinet Decision No.10 of 2019, which in turn defines the term in essence as: anyone who conducts one or several of the financial activities or operations for or on behalf of a customer. The financial activities and transactions covered are set forth in Article 2 of Cabinet Decision No.10 of 2019. "DNFBPs" are defined by reference to Cabinet Decision No.10 of 2019, which in turn defines the term in essence as: anyone who conducts one or several of the commercial or professional activities defined in Article 3 of Cabinet Decision No.10 of 2019. The said Article 3 provides the categories of persons and trade or business activities falling within the ambit of DNFBPs.

Federal Law No.20 of 2018 requires that Financial Institutions and DNFBPs shall, upon suspicion or if they have reasonable grounds to suspect a transaction or funds representing all or some proceeds, or suspicion of their relationship to Crime or that they will be used regardless of their value, to inform the UAE FIU without delay directly and provide the UAE FIU with a detailed report including all data and information available regarding that transaction and the parties involved, and to provide any additional information required by the UAE FIU, with no right to object under confidentiality provisions. Cabinet Decision No.10 of 2019 determines and provides for the rules, controls and obligations to report suspicious transactions (considered below).

Financial Institutions and DNFBPs are required under Federal Law No.20 of 2018 to: (a) identify crime risks within their scope of work as well as continuously assess, document, and update such assessment based on the various risk factors which have subsequently been established by Cabinet Decision No. 10 of 2019 (see below) and maintain a risk identification and assessment analysis with its supporting data to be provided to the Supervisory Authority (see below) upon request; (b) take the necessary due diligence measures and procedures and define their scope, taking into account various risk factors and results of the 'national risk assessment' and retain records received during the implementation of this process; (c) refrain from opening or conducting any financial or commercial transaction under an anonymous or fictitious name or by pseudonym or number, and maintaining a relationship or providing any services to it; (d) develop internal policies, controls and procedures approved by senior management to enable them to manage risks identified and mitigate them, and to review and update them continuously, and apply this to all subsidiaries and affiliates in which they hold a majority stake; (e) promptly apply directives when issued by the competent authorities in the UAE for implementing the decisions issued by the United Nations Security Council under Chapter VII of the United Nations Convention for the Prohibition and Suppression of the Financing of Terrorism and Proliferation of weapons of mass destruction, and other related directives; (f) maintain all records, documents, and data for all transactions, whether local or international, and make this information available to the competent authorities promptly upon request as stipulated in Cabinet Decision No.10 of 2019.

It may be noted that Federal Law No.20 of 2018 provides that Cabinet Decision No.10 of 2019 shall regulate the obligations of Non-Profit Organisations ("NPOs"). Cabinet Decision No.10 of 2019 covers AML related compliance matters for NPOs and matters relating to the "Supervisory Authority for Non-Profit Organisations". Matters relating to NPOs are not within the scope of this paper.

ALYIANT2YOU : Regulatory Brief

Cabinet Decision No.10 of 2019

Cabinet Decision No.10 of 2019 contains the implementing regulation of Federal Law No.20 of 2018. In the context of obligations of Financial Institutions and DNFBPs, Cabinet Decision No.10 of 2019 covers amongst other matters: (a) what activities of Financial Institutions and DNFBPs fall within the ambit of Cabinet Decision No.10 of 2019 (and Federal Law No.20 of 2018); (b) the identification and mitigation of risks by Financial Institutions and DNFBPs; (c) the requirements for Financial Institutions and DNFBPs to carry out customer due diligence; (d) identification by Financial Institutions and DNFBPs of beneficial owners of legal persons and legal arrangements; (e) identification by Financial Institutions and DNFBPs of politically exposed persons; (f) Suspicious Transaction Reports (STRs) by Financial Institutions and DNFBPs; (g) reliance on a third party by Financial Institutions and DNFBPs with respect to undertaking customer due diligence measures; (h) internal supervision and foreign branches and subsidiaries of Financial Institutions and DNFBPs; (i) appointment by Financial Institutions and DNFBPs of a compliance officer and compliance officer tasks; (j) Financial Institutions and DNFBPs obligations in connection with high-risk countries; (k) obligations of Financial Institutions and DNFBPs relating to new technologies; (l) obligations of Financial Institutions and DNFBPs with respect to record-keeping; (m) requirements for Financial Institutions (covering: correspondent banking relationships; money or value transfer services; wire transfers; and financial groups).

Regarding the subject of Sanctions, Cabinet Decision No.10 of 2019 covers the "Implementation of Security Council Resolutions" and provides that every natural or legal person shall immediately comply with the instructions of the Competent Authorities in the UAE concerning the implementation of the resolutions of the United Nations Security Council under Chapter VII of the Charter of the United Nations regarding the prevention and suppression of terrorism and terrorism financing, and the prevention and suppression of the proliferation of weapons of mass destruction and its financing, and any other related decisions. Matters related to Sanctions are considered in detail further below under the heading of Sanctions Compliance.

Several of the provisions of Cabinet Decision No.10 of 2019 discussed in this paper use various terms, including for example: "Beneficial Owner", "Business Relationship", "Crime" (discussed earlier), "Customer", "Customer Due Diligence (CDD)", "Legal Arrangement", "Politically Exposed Persons (PEPs)", and "Shell Banks". Whilst these terms and others may not be defined in this paper (nor referred to by way of capitalisation of the first letters of each term), it is necessary for parties to consider the definitions of Cabinet Decision No.10 of 2019 in the application of the provisions of Cabinet Decision No.10 of 2019.

UAE FIU

Federal Law No.20 of 2018 provides for the establishment of the UAE FIU and together with Cabinet Decision No.10 of 2019 sets out the functions and responsibilities of the UAE FIU, which includes operating as the national centre for receiving STRs and other information related to Crime. The UAE FIU has launched the 'goAML' - UAE FIU Reporting System which all Financial Institutions and DNFBPs are mandatorily required to register on. Financial Institutions and DNFBPs are required to send STRs to the UAE FIU through the 'goAML' - UAE FIU Reporting System, as well as to respond to all additional information required by the UAE FIU.

UAE NAMLCFTC

Federal Law No.20 of 2018 provides for the establishment of the UAE NAMLCFTC and sets out its functions and responsibilities, which includes coordinating with relevant authorities and referring to related international sources of information in order to identify high-risk countries in relation to money laundering and financing of terrorism and instructing the supervisory authorities to ensure the adherence to the required due diligence procedures by Financial Institutions, DNFBPs and Non-Profit Organisations which are under their supervision. For example, in March 2021 the UAE NAMLCFTC issued a decision with respect to the operational compliance relating to: (a) Article 22 of Cabinet Decision No.10 of 2019 and (b) the FATF public statements in relation to "High-Risk Jurisdictions subject to a Call for Action" and "Jurisdictions under Increased Monitoring". By way of reference, Article 22 of Cabinet Decision No.10 of 2019 contains provisions for "High-Risk Countries" and requires Financial Institutions and DNFBPs to implement enhanced customer due diligence based on the level of risk that might arise from business relationships and transactions with natural or legal persons from high-risk countries and further that Financial Institutions and DNFBPs are required to implement customer due diligence measures required by the UAE NAMLCFTC. The countries which fall under "High-Risk Jurisdictions subject to a Call for Action" are identified by the FATF public statements. Countries which

fall under "Jurisdictions under Increased Monitoring" are also identified by the FATF public statements. The UAE NAMLCFTC requires, amongst other matters, specified enhanced customer due diligence measures and countermeasures to be implemented with respect to "High-risk Jurisdictions subject to a Call for Action", along with reporting and other obligations to the UAE FIU. In the case of "Jurisdictions under Increased Monitoring", the UAE NAMLCFTC requires the implementation of customer due diligence and enhanced customer due diligence measures on a proportionate basis to the risk level that might arise from business relationships and transactions with all types of persons in the jurisdictions listed by the FATF as "Jurisdictions under Increased Monitoring". The specific requirements of the UAE NAMLCFTC should be referred to and considered with respect to the above matters, along with the further guidance issued by the UAE FIU.

Supervisory Authorities

Federal Law No.20 of 2018 along with Cabinet Decision No.10 of 2019 contain provisions for the powers and functions of Supervisory Authorities. Both define the term "Supervisory Authority" in essence as: "Federal and local authorities, which are entrusted by legislation to supervise Financial Institutions, Designated Non-Financial Businesses and Professions and Non-Profit Organisations or the competent authority in charge of approving the pursuit of an activity or a profession in case a supervisory authority is not assigned by legislation.". Cabinet Decision No.10 of 2019 contains provisions for "Supervisory Authority for Financial Institutions and DNFBPs" and provisions for "Supervisory Authority for Non-Profit Organisations". With respect to Financial Institutions and DNFBPs, there are primarily six domestic Supervisory Authorities in the UAE responsible for supervising Financial Institutions and DNFBPs falling within the jurisdictional purview of the applicable Supervisory Authority, namely: (i) the Central Bank of the UAE; (ii) the UAE Securities and Commodities Authority; (iii) the UAE Ministry of Economy; (iv) the UAE Ministry of Justice; (v) the Dubai Financial Services Authority (**"DFSA"**) of the DIFC; and (vi) the Financial Services Regulatory Authority of the ADGM.

AML Compliance in the DIFC - AML Module

At the outset, the DIFC is governed by two separate and complimentary frameworks in relation to AML regulations. These frameworks are: (a) the Federal framework (covering in present context the Federal AML Legislation) and (b) the DIFC framework (covered by the Regulatory Law 2004 and the AML Module) in the case of a "Relevant Person" in the DIFC. Regarding (a) above, it should also be noted that the UAE criminal law applies in the DIFC and therefore, persons in the DIFC are required to be aware of their obligations in respect of the UAE criminal law (including Federal AML Legislation and Federal Law No.3 of 1987). Regarding (b) above, pursuant to the Regulatory Law, the DFSA has jurisdiction for the regulation of AML matters in the DIFC relating to a "Relevant Person" and their officers, employees and agents. Accordingly, the DFSA is the "Supervisory Authority" for a "Relevant Person" in the DIFC for the purposes of the Federal AML Legislation and the AML Module.

The AML Module provides a single reference point for all "Relevant Persons" who are supervised by the DFSA for AML compliance. The AML Module applies to "every Relevant Person in respect of all its activities carried on in or from the DIFC". A "Relevant Person" is defined in the AML Module as: (a) an "Authorised Firm" other than a Credit Rating Agency; (b) an "Authorised Market Institution"; (c) a "DNFBP"; or (d) a "Registered Auditor". Each is defined in the AML Module and in other modules of the DFSA Rulebook.

The topics covered by the AML Module including the following: (i) application of a risk-based approach; (ii) business risk assessment; (iii) customer risk assessment; (iv) customer due diligence; (v) reliance on a third party, outsourcing and money service providers; (vi) correspondent banking, electronic fund transfers and audit; (vii) sanctions and other international obligations; (viii) appointment, qualities and responsibilities of a money laundering reporting officer (MLRO); (ix) AML training and awareness, (x) suspicious activity reports; (xi) a general section (dealing with groups, branches and subsidiaries; group policies; notifications; record keeping; submission of an "Annual AML Return"; communications with the DFSA; employee disclosures and decision making process); (xii) DNFBP registration and supervision. Matters related to Sanctions are considered in detail further below under the heading of Sanctions Compliance.

Several of the provisions of the AML Module discussed in this paper use various terms, including for example: "Beneficial Owner", "customer", "Customer Due Diligence (CDD)", "legal arrangement", "legal person", "natural person", "Politically Exposed Person (PEP)", and "Shell Banks". Whilst these and other terms may not be defined in

this paper (nor referred to by way of capitalisation of the first letters of each term), it is necessary for parties to consider the definitions in the AML Module in the application of the provisions of the AML Module.

Risk Based Approach

Federal Law No. 18 of 2020 along with Cabinet Decision No. 10 of 2019, and in the case of the DIFC, the AML Module, contemplate a risk-based approach towards compliance with same.

Federal Law No. 18 of 2020 and Cabinet Decision No. 10 of 2019

We had earlier in the context of Federal Law No.18 of 2020 discussed obligations of Financial Institutions and DNFBPs, including matters relating to: (a) identification of crime risks; (b) taking necessary due diligence measures; and (c) developing internal policies, controls and procedures to manage and mitigate risks. To elaborate, Cabinet Decision No.10 of 2019 requires Financial Institutions and DNFBPs to identify, assess, and understand their crime risks in concert with their business nature and size, and comply with the following: (a) consider all relevant risk factors such as customers, countries or geographic areas; and products, services, transactions and delivery channels, before determining the level of overall risk and the appropriate level of mitigation to be applied; and (b) document risk assessment operations, keeping them up to date on an on-going basis and making them available upon request. Financial Institutions and DNFBPs are required to take steps in the context of the above by: (a) developing internal policies, controls and procedures that are commensurate with the nature and size of their business and are approved by senior management, to enable them to manage the risks that have been identified, and if necessary, to monitor the implementation of such policies, controls and procedures, and update the same; (b) apply customer due diligence measures to enhance the management of high risks once identified. Financial Institutions and DNFBPs: (i) cannot deal with Shell Banks, whether to open bank accounts in their names, or to accept funds or deposits from them; and (ii) cannot create or keep records of bank accounts using pseudonyms, fictitious names or numbered accounts without the account holders name.

AML Module

The AML Module contemplates a risk-based approach and requires a Relevant Person to, amongst other matters, assess and address its AML risks by reviewing the risks to which the person is exposed as a result of the nature of its business, customers, products, services and any other matters which are relevant in context of money laundering, terrorist financing and the financing of illegal organizations and then adopting a proportionate approach to mitigate those risks. In terms of the AML Module, a Relevant Person must take appropriate steps to identify and assess money laundering, terrorist financing and the financing of illegal organizations risks to which its business is exposed (i.e. a business risk assessment), taking into account the nature, size and complexity of its activities.

When identifying and assessing such risks, the Relevant Person is required to take into account, to the extent relevant, any vulnerabilities relating to: (i) its type of customers and their activities; (ii) the countries or geographic areas in which it does business; (iii) its products, services and activity profiles; (iv) its distribution channels and business partners; (v) the complexity and volume of its transactions; (vi) the development of new products and new business practices, including new delivery mechanisms, channels and partners; and (vii) the use of new or developing technologies for both new and pre-existing products.

In terms of the AML Module, a Relevant Person must: (a) establish and maintain effective policies, procedures, systems and controls to prevent opportunities for money laundering, terrorist financing and the financing of illegal organizations in relation to the Relevant Person and its activities; (b) ensure that its systems and controls: (i) include the provision to the Relevant Person's senior management of regular management information on the operation and effectiveness of its AML compliance systems and controls necessary to identify, measure, manage and control the Relevant Person's money laundering, terrorist financing and the financing of illegal organizations risks; (ii) enable it to determine certain specified matters, including whether a customer or a beneficial owner is a politically exposed person; and if it provides a customer with a life insurance or other similar policy, whether a beneficiary of the policy, or a beneficial owner of the beneficiary, is a politically exposed person; and (iii) enable the Relevant Person to comply with the AML Module and Federal AML Legislation; and (c) ensure that regular risk assessments are carried out on the adequacy of the Relevant Person's AML compliance systems and controls.

The AML Module requires a Relevant Person to: (a) undertake a risk-based assessment of every customer; and (b) assign the customer a risk rating proportionate to the customer's money laundering, terrorist financing and financing of

illegal organisations risks. The customer risk assessment is to be completed prior to undertaking customer due diligence for new customers, and whenever it is otherwise appropriate for existing customers. The AML Module specifies the matters a Relevant Person must address when undertaking a risk-based assessment of a customer.

The AML Module provides that a Relevant Person: (a) is prohibited from establishing a business relationship with a "Shell Bank" (as defined in the AML Module); (b) must not establish or maintain an anonymous account, an account in a fictitious name, or a nominee account which is held in the name of one person but which is controlled by or held for the benefit of another person whose identity has not been disclosed to the Relevant Person; and (c) must not establish a business relationship with a customer which is a legal person or a legal arrangement if the ownership or control arrangements of the customer prevent the Relevant Person from identifying one or more of the customer's beneficial owners.

Risk rating

The development of a risk matrix based on a pre-defined set of criteria using the methodologies discussed above under Federal Law No.20 of 2018 and Cabinet Decision No.10 of 2019, and in the case of the DIFC, the AML Module, enables the allocation of an appropriate risk rating to every customer such as "low" or "high", or a sliding numerical scale such as 1 for lowest risk to 10 for the highest. Such a risk rating helps to determine how and when to apply the appropriate checks, treatment, and controls that are commensurate to the level of risk, as well as to determine the level of customer due diligence that will be required for a customer, including circumstances where simplified customer due diligence or enhanced customer due diligence are appropriate.

Customer Due Diligence

Cabinet Decision No.10 of 2019 and the AML Module contemplate that once a risk rating proportionate to the AML risks is assigned to a customer, the appropriate level of Customer Due Diligence (**"CDD"**) is to be carried out. The approach to CDD under Cabinet Decision No.10 of 2019 and the AML Module are generally aligned and which are discussed below.

Cabinet Decision No.10 of 2019

Financial Institutions and DNFBPs are required to undertake CDD measures in the following cases: (i) when establishing the business relationship; (ii) carrying out occasional transactions in favour of customers for amounts equal to or exceeding the amount prescribed in Cabinet Decision No.10 of 2019, whether the transaction is carried out in a single transaction or in several transactions that appear to be linked; (iii) carrying out occasional transactions in the form of wire transfers for amounts equal to or exceeding the amount prescribed in Cabinet Decision No.10 of 2019; (iv) where there is a suspicion of a Crime; (v) where there are doubts about the veracity or adequacy of previously obtained customer's identification data. Financial Institutions and DNFBPs are also required to undertake ongoing CDD measures and supervision of business relationships.

Financial Institutions and DNFBPs are for CDD purposes required to identify a customer's identity, whether the customer is permanent or walk-in, and whether the customer is a natural person or legal person or legal arrangement, and verify the customer's identity and identity of the beneficial owner. Identity verification is required to be done using documents, data or information from a reliable and independent source or any other source to verify the identity verification. Cabinet Decision No.10 of 2019 contains specific identity verification requirements for: (a) customers which are natural persons, legal persons and legal arrangements; and (b) beneficial owners of legal persons and legal arrangements. Cabinet Decision No.10 of 2019 sets out obligations for Financial Institutions and DNFBPs to determine and identify whether a customer or a beneficial owner are politically exposed persons under the terms of Cabinet Decision No.10 of 2019. Financial Institutions are required to take reasonable measures to determine the beneficiary or beneficial owner of life insurance policies and family takaful insurance, and are subject to prescribed obligations in connection with politically exposed persons.

The above and related matters are considered in detail in Cabinet Decision No.10 of 2019, including the timing for undertaking CDD and circumstances where simplified CDD may be carried out and circumstances where enhanced CDD measures must be carried out, such as taking reasonable measures to establish the "source of funds" of the customer and the beneficial owner. An example of enhanced CDD requirements has been provided earlier above in the

context of the decision of the UAE NAMLCFTC for countries which fall under "High-Risk Jurisdictions subject to a Call for Action" identified by FATF and for "Jurisdictions subject to Increased Monitoring" identified by FATF.

In terms of Cabinet Decision No.10 of 2019, Financial Institutions and DNFBPs are prohibited from establishing or maintaining a business relationship or executing any transaction should they be unable to undertake CDD measures with respect to a customer and should consider reporting a Suspicious Transaction to the UAE FIU. Cabinet Decision No.10 of 2019 provides that even if they suspect the commission of a Crime, Financial Institutions and DNFBPs should not apply CDD measures if they have reasonable grounds to believe that undertaking such measures would "tip-off" the customer and that they should report a Suspicious Transaction to the UAE FIU along with the reasons having prevented them from undertaking such measures.

Regarding a "Suspicious Transaction", Cabinet Decision No.10 of 2019 provides that if Financial Institutions and DNFBPs have reasonable grounds to suspect that a Transaction (defined in Cabinet Decision No.10 of 2019 as all disposal or use of funds or proceeds including for example: deposit, withdrawal, conversion, sale, purchase, lending, swap, mortgage, and donation), attempted Transaction, or funds constitute crime proceeds in whole or in part or are related to a Crime or intended to be used in such activity, regardless of the amount, the following is required to be followed: (a) directly report STRs to the UAE FIU without any delay, via the electronic system (i.e. goAML UAE FIU Reporting System) or by any other means approved by the UAE FIU; and (b) respond to all additional information required by the UAE FIU. Further, Financial Institutions and DNFBPs, their managers, officials or staff, cannot disclose, directly or indirectly, to the customer or any other person(s) that they have reported, or are intending to report a "Suspicious Transaction", nor shall they disclose the information or data contained therein, or that an investigation is being conducted in that regard. A "Suspicious Transaction" is defined by Cabinet Decision No.10 of 2019 as: "Transactions related to funds for which there are reasonable grounds to suspect that they are earned from any felony or misdemeanour related to the financing of terrorism or of illegal organisations, whether committed or attempted.".

It should be noted that Financial Institutions and DNFBPs are required to appoint a compliance officer in accordance with the provisions of Cabinet Decision No.10 of 2019 and which sets out the tasks of the compliance officer, including reviewing, scrutinising and studying records, receiving data concerning Suspicious Transactions, and taking decisions to either notify the UAE FIU or maintain the Transaction with reasons for maintaining same, while maintaining complete confidentiality.

AML Module

In connection with the DIFC, a "Relevant Person" under the AML Module is required to undertake CDD by: (a) identifying the customer and verifying the customer's identity; (b) identifying the beneficial owners of the customer and take reasonable measures to verify the identity of the beneficial owners, so that the Relevant Person is satisfied that it knows who the beneficial owners are; (c) if the customer is: a legal person or a legal arrangement, taking reasonable measures to understand the nature of the customer's business and its ownership and control structure; and (c) undertaking on-going due diligence of the customer business relationship. The AML Module sets out, amongst other matters, the obligations and requirements for CDD with respect to: a natural person; a body corporate; a foundation; an express trust or other similar legal arrangement.

The AML Module also contains requirements for the identification and verification of the beneficial owners of: a body corporate, foundation, trusts and similar arrangements, and of a life insurance policy. The AML Module provides for the requirement of a Relevant Person to determine if the customer, or a beneficial owner of a customer, is a politically exposed person; and for a life insurance or other similar policy, if the beneficiary of the policy, or a beneficial owner of the beneficiary is a politically exposed person. Guidance is provided by the AML Module on: CDD, identification and verification of beneficial owners, and on politically exposed persons, as well as other related matters pertaining to CDD, including the timing for carrying our CDD and circumstances where a Relevant Person must undertake "Enhanced customer due diligence" (e.g. including taking specified measures such as obtaining and verifying prescribed additional information and taking reasonable measures to establish the "source of funds" and "source of wealth" of a customer or if applicable of the beneficial owner) and where a Relevant Person is permitted to undertake "Simplified customer due diligence", and on-going CDD measures. As mentioned above, an example of enhanced CDD requirements has been provided earlier above in the context of the decision of the UAE NAMLCFTC for countries which fall under "High-

Risk Jurisdictions subject to a Call for Action" identified by the FATF and for "Jurisdictions subject to Increased Monitoring" identified by the FATF.

The AML Module provides that where in relation to any customer, a Relevant Person is unable to conduct or complete the requisite CDD under the AML Module, it must to the extent relevant: (a) not carry out a transaction with or for the customer through a bank account or in cash; (b) not open an account or otherwise provide a service; (c) not otherwise establish a business relationship or carry out a transaction; (d) terminate or suspend any existing business relationship with the customer; (e) return any monies or assets received from the customer; and (f) consider whether the inability to conduct or complete CDD necessitates the making of a Suspicious Activity Report (i.e. a report regarding suspicious activity (including a suspicious transaction) made to the UAE FIU under Federal Law No.20 of 2018 and Cabinet Decision No.10 of 2019 - discussed above). A Relevant Person is not required to comply with (a) to (e) above if: (i) to do so would amount to "tipping off" the customer, in breach of Federal AML Legislation; or (ii) the UAE FIU directs the Relevant Person to act otherwise.

Regarding a "Suspicious Activity Report", in terms of the AML Module, a Relevant Person is required to establish and maintain policies, procedures, systems and controls in order to monitor and detect suspicious activity or transactions in relation to potential money laundering, terrorist financing and the financing of illegal organisations. In addition to further requirements set out in the AML Module, a Relevant Person must ensure that where the Relevant Person's MLRO receives a notification pursuant to the requirements of the AML Module, the MLRO must without delay: (a) inquire into and documents the circumstances in relation to which the notification made under the AML Module was made; (b) determine whether in accordance with Federal AML Legislation, a Suspicious Activity Report must be made to the UAE FIU and documents such determination; (c) if required, make a Suspicious Activity Report to the UAE FIU as soon as practicable; and (d) notify the DFSA of the making of such Suspicious Activity Report immediately following its submission to the UAE FIU. In terms of the guidance provided by the AML Module, Relevant Persons or any of their employees must not disclose, directly or indirectly, to the customer or to any other person that they have reported, or are intending to report, a suspicious transaction or the fact that a suspicious transaction is being investigated. In terms of the guidance provided in the AML Module, if a Relevant Person reasonably believes that performing CDD measures will tip-off a customer or potential customer, it may choose not to pursue that process and should file a Suspicious Activity Report.

Sanctions Compliance

An integral and critical part of the entire AML process considered in this paper is Sanctions compliance, which is covered below in the discussion on Cabinet Decision No.74 of 2020 and the AML Module.

Cabinet Decision No.74 of 2020

Under Chapter VII of the Charter of the United Nations, the United Nations Security Council has the capacity to take measures to maintain or restore peace and security. Chapter VII provides in material part that the United Nations Security Council may decide what measures not involving the use of armed forces are to be employed to give effect to its decisions, and it may call upon the Member States of the United Nations to apply such measures. Article 41 of Chapter VII gives the United Nations Security Council the authority to use a variety of measures to enforce its decisions and among the most common are measures known as "sanctions". There are a number of ongoing United Nations sanctions regimes, with each sanction's regime administered by a sanctions committee.

The UAE is a member of United Nations and has also recently been elected to the United Nations Security Council for the term 2022-2023. As a member of the United Nations, the UAE implements United Nations Security Council resolutions, including those related to the United Nations's sanctions regimes. Through Cabinet Decision No.74 of 2020, the UAE implements relevant United Nations Security Council resolutions on the suppression and combatting of terrorism, terrorist financing and countering the financing of proliferation of weapons of mass destruction, including the implementation of targeted financial sanctions (**"TFS"**).

The terms TFS refers to asset freezing and other financial prohibitions, agreed upon by the United Nations Security Council to prevent funds or other assets from being made available, directly or indirectly, for the benefit of listed individuals, groups and entities. In the context of TFSs, **FATF Recommendations 6 and 7** are relevant. Recommendation 6 provides for *"Targeted financial sanctions related to terrorism and terrorist financing"* and pertains to countries implementing targeted financial sanctions regimes to comply with United Nations Security Council

resolutions relating to the prevention and suppression of terrorism and terrorist financing. Recommendation 7 provides for *"Targeted financial sanctions related to proliferation"* and pertains to the requirement for countries to implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.

The provisions of Cabinet Decision No.74 of 2020 or the "Decision"

The Decision repeals an earlier Cabinet Decision No.20 of 2019 covering the similar subject matter covered by the Decision. The Decision applies to all persons (natural and legal) in the UAE. Financial Institutions and DNFBPs have specific obligations under the Decision.

By way of overview, the Decision, amongst other provisions, contains detailed provisions for: proposed Listing and re-listing on Local Lists and updating of same; de-listing from Local Lists; enforcement and publication of Local Lists; grievances against decisions to list on Local Lists; lifting freezing and Other Measures in the case of false positives on Local Lists; permission to use Funds frozen pursuant to Listing on Local Lists; request to Listing on another country's list (subject to meeting the criteria under United Nations Security Council Resolution No.1373 (2001)); proposal for Listing to the Sanctions Committee; publication of the Sanctions List, Local Lists, and implementation of related decisions; declared procedures relating to the Sanctions List; freezing Funds as per the Sanctions List and Local Lists; lifting the freezing of Funds and Other Measures taken in cases of false positives on the Sanctions List; permission to use Funds frozen as per the Sanctions List; obligations of Financial Institutions and DNFBPs.

We focus on: (a) freezing Funds as per the Sanctions List and Local Lists; and (b) obligations of Financial Institutions and DNFBPs. So as to put the matters at (a) and (b) in context, discussed at the outset are the following definitions which are relevant to these two matters: "Cabinet", "Office", "Listing", "Relevant UNSCRs", "Sanctions Committee", "Listed Person", "Local Lists", "Sanctions List", and "Funds".

The "Cabinet" refers to the UAE Cabinet. "Office" (which we also refer to herein as the "Executive Office") is defined by the Decision as: "The Executive Office of the Committee for Goods Subjected to Import and Export Control". The term "Listing" is defined by the Decision as "Identifying the individual or organization subject to sanctions imposed pursuant to relevant UNSCRs, decisions of the Sanctions Committee, or the relevant decision of the Cabinet, as the case maybe, and implementing relevant sanctions against such individuals or organization, with a statement for the reasons for listing.". The term "Sanctions Committee" is defined by the Decision to mean: "Any of the UN Security Council Committees established as per its resolutions…" and the definition also specifically refers to several specific committee establishment resolutions. The term "Relevant UNSCRs" is defined as: "All current and future UN Security Council resolutions relating to the suppression and combatting of terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing, including but not limited to Resolutions 1267 (1999), 1988 (2011), 1989 (2011), 1718 (2006), 2231 (2015) and any successor resolutions.". The term "Listed Person" is defined by the Decision as a: "person or organization listed by the UNSC on the Sanctions List, or listed by the Cabinet on Local Lists, as the case maybe.".

"Local Lists" is defined by the Decision as: "Terrorism lists issued by the Cabinet pursuant to the provisions of Article 63 paragraph (1) of Federal Law No.7 of 2014.". By way of reference, Article 63(1) of Federal Law No. 7 of 2014 provides that the Cabinet may, based on the proposal of the Minister of Presidential Affairs, issue a decision on the creation of list(s) of terrorist organisations or persons that pose threat to the UAE or that the UAE is internationally bound to include therein. As mentioned earlier, the Decision provides for the procedure for proposed Listing and re-listing on Local Lists and updating of same. The "Local Lists" can be accessed through the website of the Executive Office.

The term "Sanctions List" is defined by the Decision as: "A list containing the names of individuals and organizations linked to terrorism, financing of terrorism or proliferation of weapons of mass destruction and its financing, and that are subject to sanctions imposed as per UNSCRs and decisions of the Sanctions Committee, along with information related to such persons and reasons for their listing.". The "Sanctions List" can be accessed through the website of the Executive Office or by directly visiting the website of the United Nations.

The terms "Funds" is broadly defined in the Decision as: "Assets of all types, in whatever form and however acquired, whether corporeal or incorporeal, tangible or intangible, moveable or immovable, electronic, digital or encrypted, including national currency, foreign currencies, documents and legal instruments establishing ownership of such assets or any associated rights, in whatever form, including electronic or digital forms, as well as economic resources considered as assets of any kind, including oil and natural resources, and bank credits, checks, money orders, shares, securities, bonds, drafts, and letters of credit and any interest, dividends, or other income accruing from or generated by such assets, and that may be used to obtain any other funds, goods or services including internet posting services or related services.". The TFS Guidance (discussed below) elaborates on the meaning of 'Funds' and categories of Funds.

Freezing Funds as per the Sanctions List and Local Lists

The Decision provides that any person shall "Without Delay" (which terms is defined in Cabinet Decision No.74 of 2020 and a prescribed time period for which is provided in the Decision), and without prior notice, freeze Funds as per the Sanctions List and Local Lists without limiting such measures to funds that may be used to perpetrate a certain act, conspiracy, threat or agreement related to terrorism and its financing or weapons of mass destruction proliferation and its financing. The Decision further provides that the freezing measures include the following: (a) funds owned or controlled, wholly or jointly, directly or indirectly, by the Listed Person or funds owned or controlled, wholly or jointly, directly or indirectly, by a person or organization acting on behalf of or at the direction of the Listed Person; and (b) Funds derived from funds under (a) above. The Decision prescribes the notification obligations with respect to the freezing measures taken and the time period for doing so. With respect to the above, the Guidance on TFS (discussed below) elaborates on the timelines and notification obligations applicable to Financial Institutions, DNFBPs and to any other individual or entity, which must be adhered to. Further, in terms of the Decision, no person can make funds available or provide financial or other related services whether in whole or in part, directly or indirectly, to any persons or entities on the Sanctions List or Local Lists except with the authorisation of the Office in line with the provisions of the Decision. The TFS Guidance (discussed below) elaborates further on the above matters.

Obligations of Financial Institutions and DNFBPs

The Decision provides for additional obligations which are to be complied with by "Financial Institutions" and "DNFBPs". The obligations referred to are several fold and in essence include: (i) registration on the website of the Office (i.e. the Executive Office) to receive notifications related to new listing, re-listing, updating or uploading the list and issued by the United Nations Security Council, the Sanctions Committee or the Cabinet; (ii) regularly screening their databases and transactions against names on lists issued by the United Nations Security Council, the Sanctions Committee or the Local Lists and also immediately when notified of any changes to any of such lists, provided that such screening includes the following: (a) search their customer bases; (b) search the names of parties to any transaction; (c) search for the names of potential customers; (d) search for the names of beneficial owners; (e) search for the names of persons and organizations with which they have a direct or indirect relationship; (f) continuously search their customer databases before concluding any transaction, or entering into a serious business relationship with any person to ensure that their name is not listed on the Sanctions List or the Local Lists. The Decision further requires Financial Institutions and DNFBPs to implement freezing measures, without delay, and without prior notice to the Listed Person, immediately when a match is found through the screening process referred to above.

In terms of the Decision, Financial Institutions and DNFBPs are required to immediately notify the Supervisory Authority in the following cases: (a) identification of funds and actions that have been taken as per the requirements of Relevant UNSCRs or decisions of the Cabinet regarding the issuance of Local Lists, including attempted transactions; (b) detection of any match with listed persons or entities, details of the match data and actions that have been taken as per the requirements of Relevant UNSCRs and Local Lists, including attempted transactions; (c) if it was found that one of its previous customers or any occasional customer it dealt with, is listed on the Sanctions List or the Local Lists; (d) if it suspects that one of its current or former customers, or a person it has a business relationship with is listed or has a direct or indirect relationship with the Listed Person; (e) no action has been taken due to a false positive, and the inability to dismiss such false positive through available or accessible information; (f) information relating to Funds that have been unfrozen.

Financial Institutions and DNFBPs are in terms of the Decision required: (a) to establish and effectively implement internal controls and procedures to ensure compliance with the obligations arising under the Decision; (b) establish and implement policies and procedures that prohibit staff from, directly or indirectly, informing the customer or any third

party that freezing or Other Measures shall be implemented in accordance with the provisions of the Decision; and (c) cooperate with the Office and the Supervisory Authority in verifying the accuracy of submitted information. The "Other Measures" referred to are defined in the Decision as: "Sanction measures other than freezing that must be enforced, and which may be included in Relevant UNSCRs or Cabinet Decisions regarding the issuance of Local Lists, such as prohibitions relating to travel, weapons, imports, or provisions of fuel supplies.".

Obligations of Supervisory Authorities: The Decision defines "Supervisory Authorities" as "Federal and Local authorities entrusted, as per Legislation, with the supervision of Financial Institutions and Designated Non-Financial Businesses and Professions.". The Decision provides for the obligations of Supervisory Authorities, which includes supervising, monitoring and following-up to ensure compliance with the provisions of the Decision, through onsite and offsite inspection, and imposing appropriate administrative sanctions in case of violation or failure to implement such provisions. In the DIFC, the Supervisory Authority for activities which fall under the broad umbrella of "Financial Institutions" and "DNFBPs" is the DFSA in the context of a "Relevant Person" under the AML Module discussed below.

AML Module

In the DIFC, a "Relevant Person" is required to comply with the AML Module and the Decision. The AML Module makes provision for relevant United Nations resolutions and sanctions and requires a Relevant Person to establish and maintain effective systems and controls to ensure that on an ongoing basis it is properly informed as to, and takes reasonable measures to comply with, relevant resolutions or sanctions issued by the United Nations Security Council. A Relevant Person is also required to immediately notify the DFSA in prescribed circumstances.

In addition, the AML Module also provides for obligations pertaining to government, regulatory and international findings. A Relevant Person is required to establish and maintain systems and controls to ensure that on an ongoing basis it is properly informed as to, and takes reasonable measures to comply with, any findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions issued by: (a) the government of the UAE or any government departments in the UAE; (b) the Central Bank of the UAE or the UAE FIU; (c) FATF; (d) UAE enforcement agencies; and (e) the DFSA, in connection with: (i) arrangements for preventing money laundering, terrorist financing or the financing of weapons of mass destruction in a particular country or jurisdiction, including any assessment of material deficiency against relevant countries in adopting international standards; and (ii) the names of persons, groups, organisations or entities or any other body where suspicion of money laundering or terrorist financing or the financing of weapons of mass destruction exists.

In terms of the AML Module, a Relevant Person is expected to take its own steps in acquiring relevant information from various available sources, such as, for example, from the consolidated list of financial sanctions in the UAE Cabinet, European Union Office, HM Treasury (United Kingdom) lists, and the Office of Foreign Assets Control (OFAC) of the United States Department of Treasury.

The AML Module requires ongoing sanctions screening by a Relevant Person and requires a Relevant Person to review its customers, their business and transactions against the United Nations Security Council lists and against any other relevant sanctions (e.g. unilateral sanctions imposed by other jurisdictions, which may apply to a Relevant Person's jurisdiction of origin, its business and/or customer base).

Guidance on TFS for Financial Institutions and DNFBPs – May 2021 ("TFS Guidance")

The TFS Guidance issued by the Executive Office of the Committee for Goods Subjected to Import and Export Control (the "Executive Office") elaborates on matters relating to TFS and obligations under the Decision and includes the following topics: (i) the Legal Framework; (ii) What are TFS; (iii) what is the purpose of TFS; (iv) Obligations on UAE Persons to implement TFS regimes; (v) Reporting Obligations; (vi) Enforcement of TFS; (vii) Requesting an exemption or permission to access frozen funds; (viii) Procedure to cancel or lift freezing measures; (ix) Requesting the Removal or De-listing of a Designation from the Local Terrorist List (i.e. the Local List); (x) Requesting the Removal or De-listing of a Designation from the UN List (i.e. the Sanctions List). For example, the "Obligations on UAE Persons to implement TFS regimes", include the requirements for all persons (natural and legal) in the UAE, including Financial Institutions and DNFBPs to implement TFS regimes. This would, amongst other matters, entail registering at the Executive Office website to receive email notifications and updated and timely notifications about the lifting and de-

listing of individuals or entities in the Local List and the Sanctions List. The TFS Guidance elaborates on notification obligations of and time-lines for notification by: (i) Financial Institutions and DNFBPs and (ii) any other individual or entity. The Executive Office has also issued a "TFS Mini Guide" in June 2021 titled: "Targeted Financial Sanctions Instructions for Private Sector Upon Sanctions List Update".

Training

Education and the continuous training of personnel with respect to the Federal AML Legislation and in the case of a Relevant Person in the DIFC, the AML Module, is critical for the implementation by businesses of effective polices, processes, systems and controls which comply with applicable requirements.

Cabinet Decision No.10 of 2019 contains provisions for Financial Institutions and DNFBPs to prepare, execute and document ongoing training and development programs and plans for the institution's employees on Money Laundering and the Financing of Terrorism and Financing of Illegal Organizations, and the means to combat them. This obligation falls under the tasks to be performed by a compliance officer which every Financial Institution and DNFBP is required to appoint in terms of Cabinet Decision No.10 of 2019.

In the context of the DIFC, the AML Module contains provisions for AML training and awareness by a Relevant Person of relevant Employees at appropriate and regular intervals. Under the AML Module, the responsibilities of the MLRO include establishing and maintaining an appropriate money laundering and related matters training programme and adequate awareness arrangements under the AML training and awareness requirements of the AML Module. In fact, The DFSA Rulebook - General Module (GEN Module) requires an "Authorised Firm" to ensure that an Employee who falls within a category specified in the GEN Module to remain competent by completing a minimum number of hours prescribed in the GEN Module, of continuous professional development (CPD) in each calendar year. The categories of Employees specified in the GEN Module include the MLRO of an Authorised Firm and the Authorised Firm is required to ensure that: (a) the CPD is relevant to the Employee's: (i) current role and any anticipated change in that role; and (ii) professional skill and knowledge; (b) the CPD consists of structured activities; and (c) the Employee keeps adequate records of CPD activities to be able to demonstrate that the requirements in the GEN Module have been met. The reference to "structured activities" is described in the GEN Module to mean courses, seminars, lectures, conferences, workshops, web-based seminars or e-learning requiring a commitment of thirty minutes or more.

Private Sector Outreach and Guidance

Continuous private sector outreach initiatives by the public sector and regulatory authorities is invaluable and insightful for increasing awareness and understanding the requirements of AML legislation and rules in the UAE, and consequently the private sectors role in strengthening the UAE's fight against financial and related crime.

Recent instances of such private sector outreach initiatives in the UAE include: (i) the Private Sector Outreach Sessions conducted in June 2021 by the UAE Ministry of Foreign Affairs and International Cooperation along with several Supervisory Authorities (including the DFSA) in the UAE for Offshore Financial Institutions and Offshore DNFBPs; (ii) the Counter Proliferation Financing Workshop held in November 2020 by the UAE's Executive Office of the Committee for Goods and Material Subjected to Import and Export Control; and (iii) the training course on Counter Proliferation Finance held in October 2020 by the UAE's Executive Office of the Committee for Goods and Material Subjected to Import and Export Control along with the U.S. Department of State, Kings College London, and the James Martin Center for Non-Proliferation Studies. Such initiatives go towards further enhancing the quality of AML compliance efforts.

Guidelines issued from time to time are also invaluable. Some recent examples of these are: (i) the "Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations Guidelines for Financial Institutions" – March 2021, issued by the UAE NAMLCFTC; (ii) the "Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations Guidelines for DNFBPs" – March 2021, issued by the UAE NAMLCFTC; (iii) the TFS Guidance – May 2021(discussed above); (iv) the TFS Mini Guide – June 2021 (discussed above); (iv) the "Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations Guidelines for Financial Institutions" – June 2021, Central Bank of the UAE version; and (v) the "Anti-Money Laundering & Countering Terrorist Financing Guidelines" – June 2021, which is a Joint Guidance on AML/CFT by the six "Supervisory Authorities" referred to earlier (including the DFSA of the DIFC). The Joint Guidance applies to all Financial

Institutions and DNFBPs (where applicable) licensed, registered and regulated by the Supervisory Authorities. The Joint Guidance provides contextual guidance on AML/CFT standards and common themes observed during inspections of Financial Institutions and DNFBPs.

Conclusion

With the continued growth of local and foreign investment in the UAE, along with the UAE's progressive initiatives towards ease of doing business (the UAE has also been ranked 16th out of 190 countries for ease of doing business in the World Bank Group's *"Doing Business 2020"* study), having in place robust and effective policies, systems, processes and checks which are compliant with the applicable AML legislation and rules, is the *'golden thread'* that is required to run through organisations so as to understand, capture and address relevant risks, including to name a few, risks arising from: not identifying and verifying customers and beneficial owners adequately; not determining whether a customer or a beneficial owner is a politically exposed person; the breaching of sanctions; not being uptodate with regulatory changes; and not effectively implementing regulatory changes.

We advise and assist parties in developing and implementing policies, systems, processes and checks to meet their compliance obligations with AML legislation and rules. Should you require any further information or wish to speak to a representative, please contact us at info@alyiantconsultancy.com or at +971 4 4019390.

Alyiant Consultancy Limited
Date: 8th July 2021