Appendix 1

Anti-Money Laundering and Sanctions Rulebook (AML)

*In this attachment underlining indicates new text and striking through indicates deleted text.

1. INTRODUCTION

For the meaning of capitalised terms and interpretation of other terminology, see Chapter 3.

...

1.2 Application

1.2.1 (1) Subject to (2), the AML Rulebook applies to:

...

Guidance

1. Chapters 7 to 9 of the AML Rulebook deal with customers. As a Representative Office does not have customers these chapters do not apply.

2. Chapter 10 of the AML Rulebook deals with correspondent banking, electronic transfer of funds and ~~audits~~transfers of Virtual Assets and Fiat-Referenced Tokens, as well as audit, and anonymous and nominee accounts.

...

1.3.3 (1) Responsibility for a Relevant Person's compliance with the AML Rulebook lies with every member of the Governing Body, and its Senior Management.

(2) In carrying out their responsibilities under the AML Rulebook, every member of a Relevant Person's Governing Body, its Senior Management and MLRO, as the case may be, must exercise due skill, care and diligence.

...

2. OVERVIEW AND PURPOSE OF THE AML RULEBOOK

For the meaning of capitalised terms and interpretation of other terminology, see Chapter 3.

Guidance

1. Under ~~Section~~ section 15A of FSMR, the Regulator has jurisdiction for the regulation of AML/TFS in ADGM. The AML Rulebook sets out the requirements imposed by the Regulator in addition to FSMR. The UAE criminal law applies in ADGM and, therefore, Persons in ADGM must be aware of their obligations in respect of the criminal law as well as these Rules. Relevant UAE criminal laws include Federal AML Legislation and Federal Law No. (31) of 2021 (the Penal Code of the UAE). The Rules in the AML Rulebook should not be relied upon to interpret or determine the application of the criminal laws of the UAE.

2. Federal AML Legislation applies in ADGM~~. It is amended as required and new legislation is also published. Persons in ADGM must ensure they have a current~~

~~understanding of their obligations under~~, as amended and updated from time to time. Relevant Persons must comply with Federal AML Legislation, and the Regulations and Rules of the Regulator. Section 15B(1) of FSMR requires compliance with Federal AML Legislation. A failure to comply with a provision of Federal AML Legislation may also provide evidence of failure to comply with section 15B(1) of FSMR, which may then be addressed by the exercise of the FSRA's supervisory and enforcement powers.

3. The definition of Federal AML Legislation is broad. It includes all federal legislation as may be in force relating to money laundering, terrorist financing, proliferation financing, the financing of unlawful organisations, and sanctions compliance including Targeted Financial Sanctions. ~~Particular pieces of legislation to be aware of include:~~

4. Particular ~~pieces of~~ legislation to be aware of includes:

(a) Federal Law No. (7) of 2014 regarding Combatting Terrorism Offences~~;~~.

~~(b) Federal Decree Law No. (20) of 2018 on Anti-Money Laundering, Combatting the Financing of Terrorism and Financing of Illegal Organisations;~~

~~(c) Cabinet Decision No. (10) of 2019 concerning the Implementing Regulation of Decree Law No. (20) of 2018;~~

(~~d~~b) Cabinet ~~Decision~~ Resolution No. (74) of 2020 concerning the 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.

(c) Federal Decree by Law No. (10) of 2025 Concerning Combatting Money Laundering, Terrorism Financing and Proliferation Financing (referred to in this Rulebook as the AML Law).

(d) Cabinet Resolution No. (134) of 2025 Concerning the Executive Regulations of Federal Decree by Law No. (10) of 2025 Concerning Combatting Money Laundering, Terrorism Financing and Proliferation Financing (referred to in this Rulebook as the AML Regulations).

~~3~~5. ~~The AML Rulebook has been designed to provide a primary reference point for Relevant Persons that are supervised by the Regulator for AML/TFS compliance in accordance with the scope of application outlined in Rule 1.2.1. Accordingly it applies to all Relevant Persons, but to different degrees as provided in Rule 1.2.1(2). The AML Rulebook takes into consideration the fact that Relevant Persons have differing money laundering risk profiles. A Relevant Person should familiarise itself with the AML Rulebook and assess the extent to which the Chapters and sections apply to~~This Rulebook may reference specific requirements under Federal AML Legislation. This Rulebook should not be relied on to interpret or determine the application of Federal AML Legislation. Relevant Persons should refer to Federal AML Legislation itself, and guidance issued under the Federal AML Legislation, to understand their obligations under it.

6. The AML Regulations apply specific requirements to Virtual Asset Services Providers, as defined under Federal AML Legislation . In ADGM, any entity acting as a Virtual Asset Service Provider is expected to be an Authorised Person or Recognised Body, and accordingly, no entity should act as a Virtual Asset Service Provider in ADGM without the appropriate Financial Services Permission or Recognition Order.

7. Relevant Persons should ~~also~~ ensure they are aware of, and ~~take into account~~comply with, all notices issued by the Regulator ~~as well as relevant~~and applicable decisions, guidance and guidelines issued by governmental authorities in the UAE pursuant to Federal AML Legislation.

~~4. The AML Rulebook is not intended to be read in isolation from other UAE relevant legislation or developments in international policy and best practice. To the extent applicable, Relevant Persons need to be aware of, and take into account, how these may impact the Relevant Person's day-to-day operations. This is particularly relevant when considering the Local Terrorist List and the United Nations Security Council ("**UNSC**") Resolutions which apply in ADGM, and Sanctions imposed by other jurisdictions which may apply to a Relevant Person depending on the Relevant Person's jurisdiction of origin, its business and/or customer base.~~

8. Relevant Persons should ensure they remain up to date on developments in international policy and best practice. Relevant Persons should consider how these may impact day-to-day operations. Where there is a conflict between the recommendations or guidance published by international standard-setters, the requirements of the AML Rulebook should take precedence.

Federal authorities: NAMLCFTC, FIU and EOCN

9. Federal AML Legislation gives the NAMLCFTC various competencies. Relevant Persons should comply with decisions and requirements of the NAMLCFTC, including applicable countermeasures, as required by Federal AML Legislation.

10. The AML Law gives the FIU various competencies. Relevant Persons should ensure they comply with guidance issued by the FIU issued pursuant to Federal AML Legislation, including guidance related to the filing of SAR/STRs.

11. The EOCN is the federal body responsible for administering Cabinet Resolution No. (74) of 2020, and the focal point for implementation of Targeted Financial Sanctions in the UAE in coordination with the Supreme Council of National Security. The AML Law requires Relevant Persons to implement instructions issued by the EOCN concerning Targeted Financial Sanctions. Relevant Persons should also ensure they comply with the EOCN's guidance on Targeted Financial Sanctions.

Overview

~~5~~12. Chapter 1 specifies who is ultimately responsible for a Relevant Person's compliance with the AML Rulebook. The Regulator expects the Governing Body and Senior Management of a Relevant Person to establish a robust and effective AML/TFS compliance culture for the business.

~~6~~13. Chapter 2 provides an overview of the AML Rulebook and Chapter 3 sets out the key definitions in the AML Rulebook.

~~7~~14. Chapter 4 outlines the general compliance requirements, including Group policies, notifications, record-keeping requirements ~~and~~, the annual AML Return and requirements in relation to high-risk jurisdictions.

~~8~~15. Chapter 5 explains the meaning of the risk-based approach ("RBA"), which should be applied when complying with the AML Rulebook. The RBA requires a risk-based assessment of a Relevant Person's business, in Chapter 6, and its customers, in Chapter 7. A risk-based assessment should be a dynamic process involving regular review, and the use of these reviews to establish the appropriate processes to match the levels of risk. No two Relevant Persons will have the same approach and implementation of the RBA and the AML Rulebook permits a Relevant Person to design and implement systems and controls that are appropriate to its business and customers, with the obvious caveat that such systems should be reasonable and proportionate in light of the money laundering risks. The Regulator expects the RBA to determine the breadth and depth of the Customer Due Diligence ("CDD") which is undertaken for a particular customer under Chapter 8, though the Regulator understands that there is an inevitable overlap between the risk-based assessment of the customer in Chapter 7 and CDD in Chapter 8. This overlap may occur at the initial stages of onboarding of customers but may also occur when undertaking ongoing CDD.

~~9~~16. Chapter 9 sets out where a Relevant Person may rely on a third party to undertake all or some of its CDD obligations. Reliance on third-party CDD reduces the need to duplicate CDD already performed for a customer. Alternatively, a Relevant Person may outsource some or all of its CDD obligations to a service provider. Chapter 9 also covers requirements for due diligence of business partners.

~~10~~17. Chapter 10 sets out ~~certain~~ obligations on Authorised Persons and Recognised Bodies in relation to correspondent banking, ~~wire transfers and other matters which are limited to Authorised Persons, other than a Credit Rating Agency, and Recognised Bodies and, in particular, to banks.~~electronic fund transfers, transfers of Virtual Assets and Fiat-Referenced Tokens, and audit requirements.

~~11~~18. Chapter 11 sets out a Relevant Person's obligations in relation to both Sanctions issued by the UNSC and other Sanctions, and government, regulatory and international findings in relation to money laundering, terrorist financing and the financing of weapons of mass destruction ("WMD").

~~12~~19. Chapter 12 sets out the obligation for a Relevant Person to appoint an MLRO and the responsibilities of such a Person.

~~13~~20. Chapter 13 sets out the requirements for AML/TFS training and awareness. A Relevant Person should adopt the RBA when complying with Chapter 13, so as to make its training and awareness proportionate to the money laundering risks of the business and the role of the relevant Employee(s).

~~14~~21. Chapter 14 contains the obligations applying to all Relevant Persons concerning Suspicious Activity/Transaction Reports, which are required to be made under Federal AML Legislation.

~~15~~22. Chapter 15 sets out additional obligations applying to DNFBPs, including registration and notification requirements.

~~16~~23. Chapter 16 sets out the obligations applying to Relevant Persons that are NPOs.

The UAE criminal law

24. The criminal laws of the UAE apply in ADGM. Persons in ADGM must be aware of their obligations under the criminal law and Federal AML Legislation. The Rules in the AML Rulebook should not be relied upon to interpret or determine the application of the UAE's criminal laws.

~~17~~25. Under Article ~~3 of Federal Decree By~~4 of the AML Law ~~No. 20 of 2018~~, a Relevant Person may be criminally liable for the offence of money laundering if such an activity is intentionally committed in its name or for its account. Relevant Persons are also reminded that:

(a) the failure to report suspicions of money laundering;

(b) "tipping off"; and

(c) assisting in the commission of money laundering,

may each constitute a criminal offence that is punishable under the laws of the UAE.

~~18~~26. Under Article ~~27 of Federal Decree Law No. (20) of 2018 on Anti-Money Laundering, Combatting the Financing of Terrorism and Financing of Illegal Organisations~~37 of the AML Law, Relevant Persons and their Directors and Employees are protected from criminal, civil or administrative penalty or sanction when providing any information, including confidential information, as part of a good faith report made pursuant to Federal AML Legislation to relevant regulatory bodies.

Financial Action Task Force Standards

~~19~~27. The Financial Action Task Force (~~"~~FATF~~"~~) is an inter-governmental body whose purpose is the development and promotion of international standards to combat money laundering and terrorist financing. ~~20~~ The Regulator has had regard to the FATF Recommendations in making these Rules and has determined to closely align these Rules with the FATF Recommendations, where that is deemed to be necessary and appropriate. A Relevant Person may wish to refer to the FATF Recommendations and ~~Interpretive Notes~~interpretive notes to assist it in complying with these Rules. ~~However, in the event that a FATF Recommendation or Interpretive Note conflicts with a Rule in the AML Rulebook, the relevant Rule takes precedence.~~

~~21~~28. A Relevant Person may also wish to refer to the FATF typology reports, which may assist in identifying new money laundering threats and provide information on

money laundering and terrorist and proliferation financing methods. The FATF typology reports cover many pertinent topics for Relevant Persons, including corruption, new payment methods, money laundering using trusts and Company Service Providers, and vulnerabilities of free trade zones. These typology reports can be found on the FATF website www.fatf-gafi.org.

29. The FATF has also issued guidance on Targeted Financial Sanctions. Such guidance has been issued to assist in implementing the Targeted Financial Sanctions and activity-based financial prohibitions.

Basel Committee Standards

~~22~~30. The Basel Committee on Banking Supervision has published ~~a set of~~ guidelines for banks ~~(Sound Management of Risks~~ related to ~~Money Laundering and Financing of Terrorism, January 2014)~~money laundering and terrorist financing, which are intended to supplement the FATF Recommendations. Banks ~~operating~~ in ADGM should read ~~the Basel Committee guidelines~~these Rules in conjunction with those guidelines and the FATF Recommendations ~~and in complying with these Rules~~.

~~23. In the event that any of the Basel Committee guidelines conflict with a Rule in the AML Rulebook, the relevant Rule takes precedence.~~

Wolfsberg Group

~~24~~31. The Wolfsberg Group is an association of ~~thirteen~~ global banks that has published guidance aimed at assisting financial institutions in managing money laundering risks ~~(Wolfsberg Statement Guidance on a Risk Based Approach for Managing Money Laundering Risks, March 2006) and in~~and preventing terrorist financing ~~(Wolfsberg Statement on the Suppression of the Financing of Terrorism, January 2002)~~. Banks operating in ADGM should be familiar with the relevant Wolfsberg Group ~~published~~ guidance, published in conjunction with the FATF Recommendations, and ~~in complying~~ with ~~these~~the Rules.

~~25. In the event that any part of the Wolfsberg Group published guidance conflicts with a Rule in the AML Rulebook, the relevant Rule takes precedence.~~

Sanctions

~~26~~32. The UAE, as a member of the United Nations, is required to comply with all Sanctions issued by the United Nations Security Council (UNSC). The UAE also periodically publicises its own Sanctions~~.~~, including updates to the Local Terrorist List.

33. Targeted Financial Sanctions ~~(**"TFS")**~~ are Sanctions issued by the UNSC or the UAE involving asset freezing and other financial prohibitions targeted at individuals, entities or groups ~~with the aim of combatting~~to combat terrorism and terrorist financing, and countering the proliferation of WMD.

~~27.~~ UNSC Sanctions and Sanctions issued or administered by the UAE, including Targeted Financial Sanctions, apply in ADGM~~.~~ and must be complied with by Relevant Persons ~~must comply with Targeted Financial Sanctions. Sanctions compliance is emphasised by specific obligations contained in the AML Rulebook~~

~~requiring Relevant Persons to establish and maintain effective systems and controls to comply with applicable Sanctions, including in particular Targeted Financial Sanctions, as set out in Chapter 11.~~.

~~28. The FATF has issued guidance on Targeted Financial Sanctions. Such guidance has been issued to assist in implementing the Targeted Financial Sanctions and activity-based financial prohibitions. This guidance can be found on the FATF website www.fatf-gafi.org.~~

~~29~~34. Sanctions and the import and export controls imposed or administered by other national and supranational bodies may apply or be relevant to a Relevant Person or its operations and the conduct of its business. In particular, Sanctions administered by the European Union, the U.K. ~~("**HM Treasury**")~~ and the U.S. ~~(Office of Foreign Assets Control ("**OFAC**"))~~ may need to be carefully considered. The Regulator expects a Relevant Person to consider and take positive steps to ensure compliance where required or appropriate.

35. Sanctions compliance is emphasised by specific obligations contained in the AML Rulebook requiring Relevant Persons to establish and maintain effective systems and controls to comply with applicable Sanctions including, in particular, Targeted Financial Sanctions, as set out in Chapter 11. It is important for Relevant Persons to stay up to date with applicable Sanctions in order to remain in compliance.

...

3.1.1 Further to section 15(A)(1) of FSMR, a reference in the AML Rulebook to "money laundering" ~~in lower case~~ includes terrorist financing, proliferation financing, the financing of unlawful organisations and sanctions non-compliance including non-compliance with Targeted Financial Sanctions, unless the context provides or implies otherwise.

...

3.2.1 The following terms and abbreviations bear the following meanings for the purposes of these Rules.

Term	Definition
AML ~~Rulebook~~ Law	Means ~~the Anti-~~Federal Decree by Law No. (10) of 2025 Concerning Combatting Money Laundering ~~and Sanctions Rules and Guidance Rulebook~~, Terrorism Financing and Proliferation Financing.
AML Regulations	Means Cabinet Resolution No. (134) of 2025 Concerning the Executive Regulations of Federal Decree by Law No. (10) of 2025 Concerning Combatting Money Laundering, Terrorism Financing and Proliferation Financing.

Term	Definition
AML Return	Means the return which is required to be completed by Relevant Persons in accordance with ~~AML~~Rule 4.6.
AML Rulebook	Means this Anti-Money Laundering and Sanctions Rulebook.
Anti-Money Laundering Legislation	Means: (a) Federal AML Legislation; and (b) legislation administered by the Regulator relating to combatting money laundering, including this AML Rulebook.
Body Corporate	Means any body corporate, including a limited liability partnership and a body corporate constituted under the law of a country or territory outside of ADGM.
Business Day	Means any day which is not a Saturday, Sunday or an official public holiday in the ADGM.
CNMR	Means a confirmed name match report to be filed via goAML in the prescribed format.
Company Service Provider	Means a Person that~~,~~ carries out the following services on behalf of a customer: (a) acting as a formation agent of Legal Persons; (b) acting as, or arranging for another Person to act as, a director or secretary of a company, a partner of a partnership or a similar position in relation to other Legal Persons or Legal Arrangements; (c) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other Legal Person or Legal Arrangement; or ~~(d) acting as, or arranging for another Person to act as, a trustee of an express trust or performing the equivalent function for another form of Legal Arrangement; or~~ (e) acting as, or arranging for another Person to act as, a nominee shareholder for another Person.
Correspondent Account	Means an account opened ~~on behalf of~~by a Correspondent ~~Banking Client~~Bank to receive deposits from, to make payments on behalf of or to otherwise handle financial

Term	Definition
	transactions for or on behalf of the Respondent as part of the provision of Correspondent Banking ~~Client~~services.
Correspondent Bank	Means ~~a bank in a jurisdiction other than ADGM where an Authorised Person opens~~the correspondent Financial Institution in a Correspondent ~~Account~~Banking relationship.
Correspondent Banking ~~Client~~	Means ~~a Client of an Authorised Person which uses the firm's correspondent~~the provision of banking services ~~account to clear transactions for its own customer base~~by a correspondent Financial Institution to a respondent Financial Institution and other similar relationships.
Customer Due Diligence (CDD)	~~Has the meaning given in AML 8.3~~Means customer due diligence, and includes Simplified Customer Due Diligence, Standard Customer Due Diligence and Enhanced Customer Due Diligence, as applicable.
Designated Non-Financial Business or Profession (DNFBP)	Means the ~~following~~ class of Persons who carry out any of the following businesses in ADGM: (a) a real estate agency which carries out transactions ~~with other Persons that involve the acquiring or disposing~~for or on behalf of a customer involving the buying or selling of real property; (b) a dealer in precious metals or precious stones; (c) a dealer in any saleable item of a price equal to or greater than USD15,000; (d) an accounting firm, audit firm, insolvency firm or taxation consulting firm; (e) a ~~law firm, notary firm or other independent legal business~~Legal Professional; or (f) a Company Service Provider.
Director	Means: (a) In relation to an Undertaking established under the ADGM Companies Regulations, a Person who appears on the Register of Directors maintained by the ~~ADGM~~ Registrar of Companies; (b) In relation to all other Undertakings, a Person who has been admitted to a register which has a corresponding meaning to the Register of Directors

Term	Definition
	or performs the function of acting in the capacity of a Director, by whatever name called; (c) who is employed or appointed by a Person in connection with that Person's business, whether under a contract of service or for services or otherwise; or (d) whose services, under an arrangement between that Person and a third party, are placed at the disposal and under the control of that Person.
Enhanced Customer Due Diligence ~~or~~ (Enhanced CDD)	Means undertaking ~~Customer Due Diligence and~~Standard CDD and, in addition, the enhanced measures under ~~AML~~Rule 8.4.
~~Executive Office for Control and Non-Proliferation (EOCN)~~	Means ~~the UAE federal body responsible for administering Cabinet Resolution No. (74) of 2020, as may be amended, and any subsequent resolutions and the focal point for implementation of Targeted Financial Sanctions in coordination with the Supreme Council of National Security~~the Executive Office for Control and Non-Proliferation of the UAE.
~~FFR~~Fiat-Referenced Token	~~Means a fund freeze report to be filed via goAML in the prescribed format~~Has the meaning given in section 258 of FSMR.
~~FIU~~	~~Means the Financial Intelligence Unit of the UAE.~~
Financial Crime	Includes any offence involving: (a) fraud or dishonesty; (b) misconduct in or misuse of information relating to a financial market; (c) handling the proceeds of crime; or (d) the financing of terrorism.
Financial Institution	Means: (a) (i) an Authorised Person; ~~or~~ (ii) a Recognised Body; or (~~ii~~iii) any Person that carries out as its principal business an activity which would be a

Term	Definition
	Regulated Activity or would require a Recognition Order if carried out in ADGM; and (b) that is not one of the following: (i) a governmental organisation, including the Central Bank of the UAE or its equivalent in any state; or (ii) a multilateral development bank.
~~Financial Services Regulator~~ FIU	Means ~~a regulator of financial services activities established in a jurisdiction other than ADGM~~the Financial Intelligence Unit of the UAE.
~~Jurisdictions~~Jurisdiction Subject to a Call for Action	Means ~~jurisdictions~~a jurisdiction identified by the FATF as a 'high-risk ~~jurisdictions~~jurisdiction subject to a call for action' or any equivalent list ~~of jurisdictions~~ issued by the FATF.
~~Jurisdictions~~Jurisdiction Under Increased Monitoring	Means ~~jurisdictions~~a jurisdiction identified by the FATF as a '~~jurisdictions~~jurisdiction under increased monitoring' or any equivalent list ~~of jurisdictions~~ issued by FATF.
Legal Person	Means any entity other than a Natural Person that can establish a customer relationship with a Relevant Person or otherwise own property. This can include companies, Bodies Corporate ~~or unincorporate, trusts~~, unincorporated bodies, foundations, partnerships, associations, states and governments and other ~~relevantly~~ similar entities.
Legal Professional	Means a law firm, notary firm or other independent legal business whose business is carried out in the ADGM.
~~Money Laundering Reporting Officer~~ (MLRO~~)~~	Means~~, for the purposes~~ a money laundering reporting officer appointed by a Relevant Person pursuant to Rule 12.1.1(1), and in the case of an Authorised Person ~~other than a Credit Rating Agency, the Controlled Function described in GEN 5.3.8 and for a~~or Recognised Body, ~~the Key Individual described in MIR 2.3.2~~includes a Money Laundering Reporting Officer as that term is defined in GLO.
Non-ADGM Financial Services Regulator	Has the meaning given in section 258 of FSMR.
Non-Profit Organisation (NPO)	Means ~~a Legal Person or arrangement or~~an organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural,

Term	Definition
	educational, social or fraternal purposes or for other charitable purpose.
Person	Means a person and includes any Natural Person, ~~Body Corporate or body unincorporated, including a~~any Legal Person~~, company, Partnership, unincorporated association, government or state~~ and any Legal Arrangement.
Politically Exposed Person (PEP)	Means a Natural Person: (a) ~~Means a Natural Person, and includes where relevant a family member or close associate,~~ who is or has been entrusted with a prominent public function in the UAE or elsewhere, including but not limited to, a head of state or ~~of~~ government, ~~senior officials and functionaries of an international or supranational organisation,~~a senior politician, a senior ~~government, judicial or~~governmental, military, diplomatic or judicial official, ~~ambassador,~~a senior executive of a ~~state owned~~state-owned corporation, ~~or~~ an important political party official~~,~~; or (b) who is or has been entrusted with a prominent function by an international or supranational organisation, including a member of senior management such as a director, deputy director or board member or an equivalent, but not ~~middle ranking~~middle-ranking or more junior individuals in ~~these~~ categories~~.~~ (a) or (b), and (c) that is a family member or close associate of a person falling within (a) or (b).
RBA	Means a risk-based approach, as further detailed in Chapter 5.
Registrar of Companies	Means the ADGM Registrar of Companies.
Regulated Financial Institution	A Person who does not hold a Financial Services Permission or a Recognition Order but who is authorised in a jurisdiction other than ADGM to carry on any financial service by ~~another~~a Non-ADGM Financial Services Regulator.

Term	Definition
Respondent Bank	Means the respondent Financial Institution in a Correspondent Banking relationship.
~~RBA~~	~~Means a risk-based approach, as further detailed in Chapter 5.~~
Senior Management	Means: (1) In relation to a Relevant Person, one or more individuals who, whether acting individually or collectively, have the authority to make decisions that are material to a Relevant Person's business, risk profile or regulatory standing. This may include members of the Governing Body, executive directors, senior executive officers and members of executive management. ~~Means in relation to a Relevant Person every member of the Relevant Person's executive management and includes:~~ ~~(a) for an ADGM Entity, every member of the Relevant Person's Governing Body;~~ ~~(b) for a Branch, the Person or Persons who control the day-to-day operations of the Relevant Person in ADGM;~~ ~~(c) for an auditor, every member of the Relevant Person's executive management in the UAE.~~ (2) In relation to a customer that is a Body Corporate, every member of the Body Corporate's Governing Body and the person or persons who control the day-to-day operations of the Body Corporate, including its senior executive office, chief operating officer and chief financial officer.
Shell Bank	A bank that has no physical presence in the country in which it is incorporated or licensed and which is not affiliated with a regulated financial Group that is subject to effective consolidated supervision. The presence of a local agent or low-level staff in the country does not constitute a physical presence.
Simplified Customer Due Diligence (Simplified CDD)	Means ~~Customer Due Diligence~~Standard CDD that has been modified pursuant to the operation of ~~AML~~Rule 8.5.

Term	Definition
Source of Funds	Means the origin of a customer's funds, which relate to a Transaction or service, and includes how such funds are connected to a customer's Source of Wealth.
~~Suspicious Activity/Transaction Report~~ (SAR/STR)	Means a ~~report~~suspicious activity or transaction report to be made via goAML to the FIU in the prescribed format ~~regarding suspicious activity, including a suspicious Transaction, made to the FIU via goAML~~.
Standard Customer Due Diligence (Standard CDD)	Means CDD carried out pursuant to Rule 8.3.
Targeted Financial Sanctions ~~(TFS)~~	Means financial Sanctions issued by the UNSC or the UAE against specific individuals, entities or groups ~~in order~~ to combat terrorism, terrorist financing and the proliferation of WMD, including those listed on the Local Terrorist List or the UNSC Consolidated List on this basis. Financial Sanctions include asset freezing and prohibitions on making funds or other assets or services directly or indirectly available for the benefit of the target of the relevant Sanctions.
Waiver	Means in relation to GEN 8.2, written notice provided under FSMR.

...

4.1.1 (1) A Relevant Person must establish and maintain effective AML/TFS policies, procedures, systems and controls to prevent opportunities for money laundering, in relation to the Relevant Person and its activities.

(2) A Relevant Person's AML/TFS policies, procedures, systems and controls must:

(a) ensure compliance with these Rules and Federal AML Legislation;

(b) enable suspicious Persons and Transactions to be detected and reported;

(c) ensure the Relevant Person is able to provide an appropriate audit trail of a Transaction; ~~and~~

(d) ~~ensure compliance with any other obligation in these Rules.~~adequately mitigate the risks identified pursuant to Rule 6.1.1;

(e) be approved by Senior Management;

(f) be regularly reviewed and updated; and

(g) require regular reporting to Senior Management on the operation and effectiveness of its AML/TFS policies, procedures, systems and controls.

(3) A Relevant Person must:

(a) take reasonable steps to ensure that its Employees comply with the relevant requirements of its AML/TFS policies, procedures, systems and controls.; and

(b) implement appropriate screening procedures to ensure high standards when hiring employees and, where appropriate, on an ongoing basis thereafter.

(4) A Relevant Person must review the effectiveness of its AML/TFS policies, procedures, systems and controls at least annually. The review must take into account the business risk assessment conducted under Chapter 6.

...

Guidance

1. Where appropriate, a Relevant Person should incorporate all material risks and relevant controls identified in the business risk assessment undertaken in accordance with Chapter 6, including those that might arise with the introduction of a new business practice or the introduction of new technology, within the scope of the annual review under Rule 4.1.1(4).

~~**4.1.2** If another jurisdiction's laws or regulations prevent or inhibit a Relevant Person from complying with the Federal AML Legislation (including legislation relating to Targeted Financial Sanctions) or with these Rules, the Relevant Person must immediately inform the Regulator in writing.~~

2. Employee screening procedures should be commensurate with the money laundering and terrorist financing risks associated with the role, the seniority of the position and the employee's access to customers, funds, data and systems.

...

4.2.1 (1) A Relevant Person which is an ADGM Entity must ensure that its policies, procedures, systems and controls required by Rule 4.1.1 apply to:

(a) all of its branches or subsidiaries; and

(b) all of its Group entities in ADGM.

(2) The requirement in (1) does not apply if the Relevant Person can satisfy the Regulator that the relevant branch, subsidiary or Group entity is subject to regulation, including AML/TFS regulation, by a Non-ADGM Financial Services Regulator or other competent authority in a country or jurisdiction with AML/TFS regulations which are equivalent to the standards set out in the FATF Recommendations and is supervised for compliance with such regulations.

...

4.4.2 A Relevant Person must inform the Regulator in writing as soon as possible if, in the course of its activities carried on in or from ADGM, it suspects or becomes aware that another Person outside of its business is engaged in:

(a) money laundering, contrary to relevant Federal AML Legislation;

(b) a breach of Sanctions; or

(c) acts amounting to bribery under the OECD Convention on Combatting Bribery of Foreign Public Officials in International Business Transactions.

This requirement does not apply to information or documents that are legally privileged or in the public domain.

4.4.3 If another jurisdiction's laws or regulations prevent or inhibit a Relevant Person from complying with the Anti-Money Laundering Legislation, the Relevant Person must immediately inform the Regulator in writing.

Guidance

1. Refer to the Guidance under Rule 14.2 in relation to grounds for suspicion of money laundering.

2. Relevant Persons should also take into account Rule 4.5.6 and any impact on access to relevant records without delay.

4.5 Record keeping

4.5.1 A Relevant Person must, where relevant, maintain the following records:

(a) a copy of all documents and information obtained in undertaking initial and ongoing CDD or due diligence on business partners;

(b) records, consisting of the original documents ~~or~~, electronic copies and certified copies, in respect of the customer business relationship~~,~~ including:

...

(f) the documents in Rule 4.6.1; ~~and~~

(g) the report provided by the MLRO pursuant to Rule 12.4.1; and

(~~g~~h) any other matter that the Relevant Person is expressly required to record under these Rules,

for at least six years from the date on which the notification or report was made, the business relationship ends ~~or~~, the Transaction is completed, a related investigation is concluded, or a related judgment is issued, whichever occurs last.

Guidance

A Relevant Person must comply with all applicable Rules on record keeping, regardless of whether or not it is outsourcing an element of its CDD process, see also Rule ~~9.3~~9.3.2. This includes the obligation for the Relevant Person to maintain a copy of all documents obtained during initial and ongoing CDD. Where using eKYC for CDD, the Relevant Person should retain all the necessary data gathered during biometric authentication to ensure compliance with applicable Rules.

4.5.2 A Relevant Person must immediately provide to the Regulator, upon request, or a law enforcement agency, pursuant to a valid and enforceable request or requirement, a copy of the ~~record~~records referred to in Rule 4.5.1.

...

4.5.6 A Relevant Person must:

(a) identify where there is secrecy or data protection legislation that might restrict access without delay to the records referred to in Rule ~~4.6.1~~4.5.1 by the Relevant Person, the Regulator or the law enforcement agencies of the UAE; and

(b) where such legislation exists, obtain without delay certified copies of the relevant records and keep such copies in a jurisdiction which allows access by those persons in (a).

~~**4.5.7** A Relevant Person must be able to demonstrate that it has complied with the training and awareness requirements in Chapter 13 through appropriate measures, including the maintenance of relevant training records.~~

~~**Guidance**~~

~~The Regulator considers that "appropriate measures" in Rule 4.5.7 may include the maintenance of a training log setting out details of:~~

~~(a) the dates when the training was given;~~

~~(b) the nature of the training; and~~

~~(c) the names of Employees who received the training.~~

4.6 Annual AML Return

4.6.1 A Relevant Person must complete the prescribed AML Return form and submit it to the Regulator by the end of April each year, except where the Relevant Person was licensed or authorised on or after 1 November of the preceding year. The AML Return must cover the period from 1 January to 31 December of the preceding year.

Guidance

~~1. The Regulator may grant a Waiver where a Relevant Person was licensed or authorised, as applicable, on or after 1 November of the relevant reporting year.~~

~~2.~~ FEES 1.2.7 sets out the fees payable for late submission of Regulatory Filings. In addition to the imposition of a fee, the Regulator may take further action.

...

4.8.1 A Relevant Person must ~~ensure that it does~~ not prejudice an Employee who discloses any information regarding money laundering to the Regulator or to any other relevant body involved in the prevention of money laundering.

...

4.9 High Risk Jurisdictions

4.9.1 A Relevant Person must maintain up-to-date lists of Jurisdictions Under Increased Monitoring and Jurisdictions Subject to a Call for Action, and screen against them as part of a customer risk assessment undertaken pursuant to Chapter 7 and CDD undertaken pursuant to Chapter 8.

4.9.2 A Relevant Person must not establish a branch or representative office in a Jurisdiction Subject to a Call for Action.

4.9.3 All Relevant Persons must comply with their internal reporting mechanisms on monitoring transactions and activities related to Jurisdiction Subject to a Call for Action pursuant to Chapter 14, and submit suspicious transaction reporting to the FIU using the appropriate templates in goAML where relevant pursuant to Federal AML Law.

4.9.4 A Relevant Person must not rely on a Person that is incorporated in or operating from a Jurisdiction Subject to a Call to Action to conduct one or more of the elements of CDD on its behalf pursuant to Rule 9.1.1.

Guidance

Customer exposure to Jurisdictions Under Increased Monitoring and Jurisdictions Subject to a Call for Action may present higher money laundering risks and so require risk-based countermeasures. As set out in Chapter 7, in the case of customer exposure to Jurisdictions Under Increased Monitoring, this may include undertaking Enhanced CDD depending on the level of risk. Pursuant to Rule 7.1.2(2), where customers are exposed to Jurisdictions Subject to a Call for Action, Enhanced CDD must always be undertaken.

...

5.1.1 A Relevant Person must:

(a) assess and address its money laundering risks under the AML Rulebook by reviewing the risks to which the Relevant Person is exposed as a result of the nature

of its business, customers, products, services and any other matters which are relevant in the context of money laundering; and

...

Guidance

1. Rule 5.1.1 requires a Relevant Person to adopt an approach to AML/TFS which is proportionate to the risks. This is called the "risk-based approach" ("RBA"). The Regulator expects the RBA to be a key part of the Relevant Person's AML/TFS compliance culture and to cascade down from the Senior Management to the rest of the organisation. Embedding the RBA within its business allows a Relevant Person to make decisions and allocate AML/TFS resources in the most efficient and effective way.

2. In implementing the RBA, a Relevant Person is expected to have in place processes to identify, assess, monitor, manage and mitigate money laundering risks. The general principle is that where there are higher risks of money laundering, a Relevant Person is required to take enhanced measures to manage and mitigate those risks. Correspondingly, when the risks are lower, simplified measures are permitted. Simplified measures are not permitted where there is a suspicion of money laundering.

3. The RBA should not be seen as a "tick-box" approach to AML/TFS. Instead, a Relevant Person is required to assess relevant money laundering risks and adopt a proportionate response to such risks~~;~~; however, even where a customer is assessed through the RBA as being ~~low-risk~~low risk, a minimum of ~~simplified~~Simplified CDD must be undertaken in relation to that customer.

4. In adopting an RBA, a Relevant Person should continue to meet the requirements that are mandated under the AML Rulebook, including:

   (a) assessing the relevant money laundering risks in accordance with Chapter 6 or Chapter 7 of AML (as applicable);

   (b) undertaking Standard CDD in accordance with Rule 8.3.1;

   (c) undertaking Enhanced CDD pursuant to Rule 8.1.1(3) in accordance with Rule 8.4.1; and

   (d) undertaking Simplified CDD in accordance with Rule 8.5.1 where permissible pursuant to Rule 8.1.1(4).

...

6.1.1 A Relevant Person must:

(a) take appropriate steps to identify and assess money laundering risks to which its business is exposed, taking into consideration the nature, size and complexity of its activities, and have its risk assessment approved by Senior Management. Relevant Persons must take into account that money laundering risks include the risk of terrorist financing, proliferation financing, the financing of unlawful

organisations and sanctions non-compliance including non-compliance with Targeted Financial Sanctions~~.~~;

(b) when identifying and assessing the risks in (a), 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 business practices, including new delivery mechanisms, channels and partners;

(vii) the use of new or developing technologies for both new and pre-existing products and services; ~~and~~

(viii) outcomes of the national risk assessment;

(c) take appropriate measures to ensure that any risk identified as part of the assessment in (a) is taken into account in its day-to-day operations and is mitigated, including in relation to:

(i) the development of new products;

(ii) the taking on of new customers; and

(iii) changes to its business profile.

6.1.2 A Relevant Person must use the information obtained in undertaking its business risk assessment to:

(a) develop and maintain its AML/TFS policies, procedures, systems and controls as required by Rule ~~6.2.1~~4.1.1;

(b) ensure that its AML/TFS policies, procedures, systems and controls adequately mitigate the risks identified as part of the assessment in Rule 6.1.1;

(c) assess the effectiveness of its AML/TFS policies, procedures, systems and controls ~~as required by Rule 6.2.1(c)~~in order to understand the residual level of money laundering risk remaining after applying its AML/TFS systems and controls;

(d) assist in the allocation and prioritisation of AML/TFS resources; and

(e) assist in the carrying out of the customer risk assessment under Chapter 7.

6.1.3 A Relevant Person must keep its business risk assessment up to date on an ongoing basis.

~~**6.1.3** Without limiting compliance with Rules 6.1.1 and 6.1.2, prior to~~

6.1.4 Before launching any new product, service, or business practice, ~~or~~ using a new or developing technology, expanding into new markets or geographies or making changes to its customer base, a Relevant Person must take reasonable steps to ensure that it has:

(a) assessed and identified the relevant money laundering risks ~~relating to the product, service, business practice or technology~~; and

(b) taken appropriate steps to mitigate or eliminate the risks identified under (a) and assessed the residual risk.

6.1.5 A Relevant Person must ensure that regular risk assessments are carried out on the adequacy of the Relevant Person's AML/TFS systems and controls to enable it to identify, assess, monitor and manage money laundering risk adequately and are comprehensive and proportionate to the nature, scale and complexity of its activities.

Guidance

1. Unless a Relevant Person understands the money laundering risks to which it is exposed, it cannot take appropriate steps to prevent its business from being used for the purposes of money laundering. Money laundering risks vary from business to business depending on the nature of the business, the type of customers a business has, the nature of the products and services sold, and the geographical operations in which it operates.

2. The frequency of risk assessments will depend on the nature, size and complexity of the Relevant Person's business and also on when any material changes are made to its business. Keeping a business risk assessment up to date on an ongoing basis includes reviewing and updating the business risk assessment whenever necessary in response to changes to the business or external events, including those set out in 6.1.1(b)(i)-(viii) and 6.1.1(c)(i)-(iii). The Regulator expects that a Relevant Person will review and update its business risk assessment at least annually.

~~2~~3. Using the RBA, a Relevant Person should assess its own vulnerabilities to money laundering and take all reasonable steps to eliminate or manage such risks and then assess and understand the residual money laundering risk. The results of this assessment will also feed into the Relevant Person's risk assessment of its customers under Chapter 7. The business risk assessment should include identifying risks, assessing relevant controls and quantifying the residual risk.

~~3~~4. In addition to assessing risk arising from money laundering, a business risk assessment should assess the potential exposure of a Relevant Person to other Financial Crime, such as fraud and the theft of personal data. The business risk assessment should also address the Relevant Person's potential exposure to cyber security risk, as this risk may have a material impact on the Relevant Person's ability to prevent Financial Crime.

~~4~~5. A Relevant Person should, as a ~~separate and distinct~~clearly identifiable element ~~of~~within its overall business risk assessment, undertake a Targeted Financial Sanctions risk assessment ~~in order~~ to identify, understand, assess and mitigate

those risks. This should include conducting a proliferation financing and terrorist financing risk assessment.

~~5~~6. A Relevant Person should, prior to launching any new product, service or business practice, pay specific attention to assessing the potential for risks associated with all applicable aspects of Financial Crime. This is especially important given the innovative nature of any such new offering as the Relevant Person may be less familiar with the functioning of the offering, compared to existing offerings.

~~6~~7. Similarly, in using a new or developing technology, such as those associated with the Regulated Activity of Developing Financial Technology Services within the RegLab or when undertaking NFTF business, a Relevant Person should pay specific attention to assessing the potential for risks associated with Financial Crime that might arise as a result of implementing that innovative technology. For example, while the use of eKYC Systems may reduce the risk of impersonation fraud at customer onboarding, NFTF interaction with the customer may increase the risk of Financial Crime after a business relationship has been established, through transaction fraud, money laundering or theft of digitally stored CDD documentation.

~~7~~8. A business risk assessment ~~under Rule 6.1.1(b)~~ should include an assessment of the risks associated with the carrying on of NFTF business, particularly the use of eKYC Systems. The assessment should consider incorporating any relevant mitigation measures identified by the Regulator, a competent authority of the UAE, FATF, and any other relevant bodies.

9. External events that may require a Relevant Person to review and update its business risk assessment include emerging money laundering risks or typologies, changes in the regulatory environment or the guidance issued by international standard-setters, findings from audits or supervisory feedback, including the outcomes of thematic reviews, and updates to the UAE's national risk assessment.

~~**6.2 AML/TFS systems and controls**~~

~~**6.2.1** A Relevant Person must:~~

~~(a) establish and maintain effective policies, procedures, systems and controls to prevent opportunities for money laundering in relation to the Relevant Person and its activities;~~

~~(b) ensure that its systems and controls in (a):~~

~~(i) include the provision to the Relevant Person's Senior Management of regular management information on the operation and effectiveness of its AML/TFS systems and controls necessary to identify, measure, manage and control the Relevant Person's money laundering risks;~~

~~(ii) enable it to determine whether a customer or a Beneficial Owner is a PEP;~~

(iii) enable the Relevant Person to comply with these Rules and Federal AML Legislation; and

(iv) enable the Relevant Person to comply with the Penal Code; and

(c) ensure that regular risk assessments are carried out on the adequacy of the Relevant Person's AML/TFS systems and controls to ensure that they continue to enable it to identify, assess, monitor and manage money laundering risk adequately, and are comprehensive and proportionate to the nature, scale and complexity of its activities.

Guidance

1. In Rule 6.2.1(c) the frequency of risk assessments will depend on the nature, size and complexity of the Relevant Person's business and also on when any material changes are made to its business. The risk assessments should also take into account a range of financial crime, including fraud, bribery and corruption.

2. The risk assessment under Rule 6.2.1(c) should identify actions to mitigate risks associated with undertaking NFTF business generally, and the use of eKYC specifically. This is because distinct risks are often likely to arise where business is conducted entirely in an NFTF manner, compared to when the business relationship includes a mix of face-to-face and NFTF interactions. The assessment should make reference to risk mitigation measures recommended by the Regulator, a competent authority of the UAE, FATF, and other relevant bodies.

7. CUSTOMER RISK ASSESSMENT

Guidance

1. This Chapter prescribes the risk-based assessment that must be undertaken by a Relevant Person on a customer and the proposed business relationship, Transaction or product. The outcome of this process is to produce a risk rating for a customer, which determines the level of CDD that must be undertaken in relation to that customer under Chapter 8. Chapter 8 prescribes the requirements of CDD, Enhanced CDD for high-risk customers and, where appropriate, Simplified CDD for low-risk customers.

2. CDD in the context of AML/TFS refers to the process of identifying a customer, verifying such identification and monitoring the customer's business and the potential for any money laundering risk on an ongoing basis. CDD is required to be completed following a risk-based assessment of the customer and the proposed business relationship, Transaction or product.

3. Relevant Persons should note that the ongoing CDD requirements in Rule 8.6.1 require a Relevant Person to review a customer's risk rating to ensure that it remains appropriate in light of the potential money laundering risks.

~~4. The risk-based assessment of the customer and the proposed business relationship, Transaction or product required under this Chapter is required to be undertaken prior to the establishment of a business relationship with a customer. Because the risk rating assigned to a customer resulting from this assessment determines the level of CDD that must be undertaken for that customer, this process must be completed before the CDD is completed for the customer. The Regulator is aware that in practice there will often be some degree of overlap between the customer risk assessment and CDD. For example, a Relevant Person may undertake some aspects of CDD, such as identifying Beneficial Owners, when it performs a risk assessment of the customer. Conversely, a Relevant Person may also obtain relevant information as part of CDD which has an impact on its customer risk assessment. Where information obtained as part of CDD of a customer affects the risk rating of a customer, the change in risk rating should be reflected in the degree of CDD undertaken.~~

7.1 Assessing the money laundering risks of a customer

7.1.1 (1) A Relevant Person must:

(a) undertake a risk-based assessment of every customer; and

(b) assign the customer a risk rating proportionate to the assessed money laundering risks associated with the customer.

(2) The customer risk assessment in (1) must be completed~~:~~ before establishing a business relationship with a customer. The customer risk assessment for existing customers must be refreshed as part of ongoing CDD in accordance with Rule 8.6.1(e).

~~i. (a) prior to establishing a business relationship with a customer;~~

~~(b) on a periodic basis, in accordance with Rule 8.6.1(e); and~~

~~(c) whenever it is otherwise appropriate for existing customers, including where the Relevant Person becomes aware of any change to the risk factors associated with the customer that might contribute to the potential for money laundering risk to increase materially.~~

(3) When undertaking a risk-based assessment of a customer ~~under 7.1.1(1)(a)~~, a Relevant Person must identify, assess and consider:

...

Guidance

1. The purpose of a customer risk assessment is to produce a risk rating for a customer, which determines the level of CDD that must be undertaken in relation to that customer under Chapter 8.

2. The customer risk assessment should be undertaken before establishing a business relationship with that customer, as it determines the level of CDD that must be undertaken – Simplified CDD, Standard CDD or Enhanced CDD. In practice, there may be some overlap between the customer risk assessment and CDD. For example, a Relevant Person may obtain relevant information as part of CDD that affects its customer risk assessment. Where information obtained as part of a customer's CDD affects the customer's risk rating, the change in risk rating should be reflected in the degree of CDD undertaken.

7.1.2 (1) When undertaking a risk-based assessment of a customer and considering whether or not to assign a high-risk rating under 7.1.1(1)(b), a Relevant Person must take into account all relevant risk factors that would reasonably apply to the customer, including but not limited to:

(a) customer risk factors, including whether the:

(i) business relationship is conducted in unusual circumstances;

(ii) customer is resident, established, registered or conducts business in a geographical area or jurisdiction of high risk (as set out in ~~paragraph~~ (c));

...

~~(2) For the purposes of 7.1.2(1)(c), a credible source includes, but is not limited to, mutual evaluations, detailed assessment reports or follow-up reports issued by FATF, the International Monetary Fund ("**IMF**"), the World Bank, the OECD and other International Organisations.~~

(2) Where:

(a) a Jurisdiction Subject to a Call for Action is relevant to the customer;

(b) a customer is a foreign PEP or has a Beneficial Owner that is a foreign PEP; or

(c) a customer seeks to engage in or is engaged in Transaction(s) involving an unhosted wallet, as that term is defined in Rule 10.3,

the customer must be given a high-risk rating.

(3) Where:

(a) a customer is a domestic PEP or has a Beneficial Owner that is a domestic PEP; or

(b) a customer is a PEP in relation to an international or supranational organisation, or has a Beneficial Owner that is a PEP on that basis; and

(c) having undertaken appropriate risk assessments and CDD, the customer relationship is assessed as higher risk,

the customer must be given a high-risk rating.

7.1.3 (1) When undertaking a risk-based assessment of a customer and considering whether or not to assign a low-risk rating under 7.1.1(1), a Relevant Person must take into account all relevant risk factors that would reasonably apply to the customer, including but not limited to:

(a) customer risk factors, including whether the customer is:

(i) a public body or a publicly owned enterprise;

(ii) resident, established, registered or conducts business in a geographical area or jurisdiction of lower risk (as set out in ~~paragraph~~ (c));

...

~~(2)~~

7.1.4 For the purposes of Rules 7.1.2(1)(c)(i)-(ii) and 7.1.3(1)(c)(i)-(ii), a credible source includes, but is not limited to, mutual evaluations, detailed assessment reports or follow-up reports issued by FATF, the IMF, the World Bank, the OECD and other International Organisations.

Guidance on the customer risk assessment

1. The risk assessment of a customer requires a Relevant Person to allocate an appropriate risk rating to the customer. Risk ratings should be either descriptive, such as "low", "medium" or "high", or a sliding, ordinal numeric scale such as 1 for the lowest risk to 10 for the highest, with at least three differentiated risk ratings. All the factors set out in both 7.1.2 and 7.1.3 should be considered in order to assess and allocate the appropriate risk rating to the customer.

2. Depending on the outcome of a Relevant Person's assessment of its customer's money laundering risk, a Relevant Person should decide ~~to~~ what ~~degree~~level of CDD will need to be performed – Simplified CDD, Standard CDD or Enhanced CDD. For a customer exhibiting significant potential risk for money laundering ~~the~~, a Relevant Person is required to carry out Enhanced CDD under Rule 8.4, ~~in addition to the normal CDD required under Rule 8.3. For a~~which encompasses Standard CDD together with additional CDD requirements. For a customer rated low risk, the Relevant Person may be able to carry out Simplified CDD under Rule 8.5. For ~~any~~all other ~~customer~~customers, the Relevant Person must undertake Standard CDD under Rule 8.3.

3. Using the RBA, a Relevant Person could, when assessing two customers with near identical risk profiles, consider that one is high-risk and the other low-risk. This may occur, for example, where both customers may be undertaking the same high-risk activity, but one customer may be a customer in relation to a low-risk product, or may be a long-standing customer of a Group company which has been introduced to the Relevant Person.

4. Rule 4.9.1 requires screening against up-to-date lists of Jurisdictions Under Increased Monitoring and Jurisdictions Subject to a Call for Action as part of a customer risk assessment and CDD.

...

7.2.1 A Relevant Person must not establish a business relationship with a prospective customer that is a Legal Person or Legal Arrangement if the ownership or control arrangements of the customer ~~prevents~~prevent the Relevant Person from identifying one or more of the customer's Beneficial Owners.

...

7.2.3 A Relevant Person must not knowingly 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 true identity has not been disclosed to the Relevant Person.

Guidance

1. In Rule 7.2.1, ownership arrangements which may prevent the Relevant Person from identifying one or more Beneficial Owners include bearer shares and other negotiable instruments in which ownership is determined by possession.

2. A ~~Shell Bank is a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial Group that is subject to effective consolidated supervision. The Regulator does not consider that the existence of a local agent or low-level staff constitutes physical presence.~~Relevant Person should not permit a customer to use the Relevant Person's products and services to engage in business with a Shell Bank.

...

8.1.1 (1) A Relevant Person that is an Authorised Person or a Recognised Body must undertake CDD under Rule 8.3.1 where the Relevant Person:

(a) establishes a business relationship with a customer;

(b) carries out an occasional Transaction for a customer that is of an amount equal to or more than USD15,000;

(c) suspects a customer of, or a Transaction to be for the purposes of, money laundering; or

(d) doubts the veracity or adequacy of any documents or information previously provided by, or obtained for, a customer in relation to (a), (b) or (c) above.

(2) A Relevant Person that is a DNFBP must undertake CDD under Rule 8.3.1 where it:

(a) is a real estate agency and it prepares for or is involved in a Transaction, or the provision of real estate agency services to a Person, that involves the buying and selling of real property;

(b) is a dealer in precious metals or precious stones and it is involved in a Transaction in cash that amounts to USD15,000 or more, ~~whether or not the Transaction is executed in a single operation or in~~or several

~~operations~~Transactions that are or appear to be linked amounting to USD15,000 or more;

(c) is a dealer in any saleable item of a price equal to or greater than USD15,000 and it is involved in a Transaction in cash that amounts to USD15,000 or more, ~~whether or not the Transaction is executed in a single operation or in~~or several ~~operations~~Transactions that are or appear to be linked amounting to USD15,000 or more;

(d) is an accounting firm, audit firm, insolvency firm or taxation consulting firm and it prepares for or is involved in the provision of accounting, auditing, insolvency or taxation consulting services to a Person;

(e) is a law firm, notary firm or other independent legal business and it prepares for or is involved in the provision of legal or notarial services to another Person participating in financial or real property Transactions concerning the following activities:

(i) the buying and selling of real property;

(ii) the managing of client money, securities or other assets;

(iii) the management of bank, savings or securities accounts;

(iv) the organisation of contributions for the creation, operation or management of companies; or

(v) the creation, operation or management of legal persons or arrangements, and buying and selling of business entities;

(f) is a Company Service Provider and it prepares for or is involved in the provision of any of the following services to another Person:

(i) acting as a formation agent of Legal Persons or Legal Arrangements;

(ii) acting as, or arranging for another Person to act as, a director or secretary of a company, a partner of a partnership, or a similar position in relation to other Legal Persons or Legal Arrangements;

(iii) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other Legal Person or Legal Arrangement; or

~~(iv) acting as, or arranging for another Person to act as, a trustee of an express trust or performing the equivalent function for another form of Legal Arrangement; or~~

(v) acting as, or arranging for another Person to act as, a nominee shareholder for another Person~~.~~;

(g) suspects a customer of, or a Transaction to be for the purposes of, money laundering; or

(h) doubts the veracity or adequacy of any documents or information previously provided by, or obtained for, a customer in relation to (a)-(f) above.

(3) In addition to undertaking Standard CDD in accordance with Rule 8.3.1, a Relevant Person must undertake Enhanced CDD in accordance with Rule 8.4.1 for each of its customers assigned a high-risk rating;

(4) A Relevant Person may undertake Simplified CDD in accordance with Rule 8.5.1 by modifying the Standard CDD undertaken in accordance with Rule 8.3.1 for any customer assigned a low-risk rating.

Guidance

1. Providing Trust Services is a Regulated Activity pursuant to FSMR. Any Person conducting that Regulated Activity is required to be an Authorised Person and comply with the requirements applicable to Authorised Persons rather than DNFBPs.

2. Relevant Persons that are Payment Service Providers should be aware of the prohibition in COBS 19.7.1 that prevents accepting and distributing physical cash in the form of banknotes and coins to and from any Payment Service User directly or indirectly other than via an appropriately regulated Financial Institution.

~~1~~3. Relevant Persons are reminded that they are required to comply with notices and guidance issued pursuant to Federal AML Legislation in relation to CDD, including those issued by the FIU relating to CDD and filings required in goAML.

4. Relevant Persons should be aware of and comply with any restrictions on dealing in cash that are applicable to their business in ADGM, including pursuant to legislation administered by the Registrar of Companies.

5. Refer to the Guidance under Rule 14.2 in relation to grounds for suspicion of money laundering.

~~2~~6. The FIU has issued guides that require:

(a) a DNFBP that is a dealer in precious metals or precious stones to obtain relevant identification documents, such as passport, emirates ID, trade licence, as applicable, and register the information via goAML for all cash transactions equal to or exceeding USD15,000 with individuals and all cash or wire transfer transactions equal to or exceeding USD15,000 with entities. The Regulator expects a dealer in any saleable item or a price equal to or greater than USD15,000 to also comply with this requirement;

(b) a DNFBP that is a real estate agent to obtain relevant identification documents, such as passport, emirates ID, trade licence, as applicable, and register the information via goAML for all sales or purchases of Real Property where:

(i) the payment for the sale/purchase includes a total cash payment of USD15,000 or more whether in a single cash payment or multiple cash payments;

(ii) the payment for any part or all of the sale/purchase amount includes payment(s) using ~~Virtual Assets~~virtual assets;

(iii) the payment for any part or all of the sale/purchase amount includes funds that were converted from or to a ~~Virtual Asset~~virtual asset.

8.1.2 (1) A Relevant Person must also apply CDD measures to each existing customer under Rules 8.3.1, 8.4.1 or 8.5.1 as applicable:

(a) with a frequency appropriate to the outcome of the risk-based approach taken in relation to each customer; and

(b) when the Relevant Person becomes aware that any circumstances relevant to its risk assessment for a customer have changed.

(2) For the purposes of ~~8.1.2~~(1), in determining when it is appropriate to apply CDD measures in relation to existing customers, a Relevant Person must take into account, amongst other things:

(a) any indication that the identity of the customer, or the customer's Beneficial Owners, has changed;

(b) any Transactions that are not reasonably consistent with the Relevant Person's knowledge of the customer;

(c) any change in the purpose or intended nature of the Relevant Person's relationship with the customer; or

(d) any other matter that might affect the Relevant Person's risk assessment of the customer.

Guidance

1. A Relevant Person should undertake appropriate CDD in a manner proportionate to the customer's money laundering risks. This means that all customers are subject to Standard CDD under Rule 8.3.1. However, for high-risk customers, additional Enhanced Customer Due Diligence measures should also be undertaken under Rule 8.4.1. For customers having a low-risk rating, the requirements under Rule 8.3.1 may be modified according to the assessed risk to Simplified CDD, in accordance with Rule 8.5.1.

2. The frequency for undertaking CDD for existing customers will be determined by the risk rating assigned to a particular customer. The Regulator expects that customers rated high risk for money laundering should be reviewed more frequently than customers rated lower risk for money laundering.

3. A Relevant Person should undertake CDD to guard against a range of money laundering risks as well as a range of financial crime risks, including fraud.

8.2 Timing of Customer Due Diligence

8.2.1 ~~(1)~~ ~~For a~~A Relevant Person ~~that is an Authorised Person or Recognised Body~~must undertake CDD as required by Rule 8.1.1 at the following times (as applicable):

~~(a) the appropriate CDD obligations, subject to (1)(b), must be fulfilled before the Relevant Person undertakes any Transaction on behalf of the customer or when undertaking an occasional transaction under 8.1.1(1)(b).~~

~~(b) the Relevant Person does not have to fulfil the verification of the identity of a customer and Beneficial Owners obligations under the AML Rules before undertaking a Transaction for a customer or occasional transaction where it has, on reasonable grounds, established that:~~

(~~i~~a) ~~there is little risk of money laundering and that risk is effectively managed; and~~when it is establishing the relevant business relationship with the customer;

(~~ii~~b) ~~doing so would interrupt or delay the normal course of business in respect of effecting the~~before carrying out the relevant Transaction~~.~~ or services; or

~~(2)~~ ~~(a) A Relevant Person that is a DNFBP must fulfil the appropriate CDD and reporting obligations where applicable before the Relevant Person prepares for or carries out a Transaction or provision of a service in Rule 8.1.1(2)(a), (d), (e) or (f).~~

(c) when the suspicion or doubt arises for the purposes of Rules 8.1.1(1)(c)-(d) and 8.1.1(2)(g)-(h), before carrying out any further business, Transactions or services,

except as provided in Rules 8.2.2 and 8.3.1(2).

8.2.2 (~~b~~1) A Relevant Person ~~that is a DNFBP as a result of carrying on one or more of the business activities referred to in Rule 8.1.1(2)(b) or (c) must fulfil the appropriate CDD and reporting obligations where applicable before the Relevant Person prepares for or carries out a transaction that includes a total cash payment of USD15,000 or more, whether in a single cash payment or multiple cash payments.~~may establish the business relationship or carry out the Transaction or the service, as contemplated by Rule 8.1.1, without completing verification of the identity of the customer and any Beneficial Owner(s) in accordance with Rule 8.2.1(a) and (b) if the following conditions are met:

~~2.~~ ~~(3) The Relevant Person does not have to fulfil the verification of the identity of a customer and Beneficial Owners obligations under the AML Rules preparing for or carrying out a Transaction for its customer concerning those business activities referred to in Rule 8.1.1(2) where it has, on reasonable grounds, established that:~~

(~~i~~a) there is little risk of money laundering, and ~~that~~any such risk is effectively managed; ~~and~~

(~~ii~~b) ~~doing so would~~deferral of verification is necessary in order not to interrupt ~~or delay~~ the normal course of business ~~in respect of effecting the Transaction.~~; and

~~(4) A Relevant Person that has relied on Rule 8.2.1(1)(b) or 8.2.1(3) must fulfil its CDD obligations as soon as practicable after effecting the Transaction.~~

(c) subject to (2), the relevant verification is completed as soon as possible and in any event no later than 20 Business Days after the business relationship is established, or the transaction or services have commenced (as applicable).

(~~5~~2) Where ~~the~~a Relevant Person, having relied on Rule 8.2.1~~(1)(b) or 8.2.1(3) is unable to complete the verification of the identity of a customer and any Beneficial Owners within twenty Business Days of effecting a Transaction or occasional transaction~~, is unable to comply with the verification requirement in Rule 8.2.2(1)(c) before the end of the 20 Business Day period, it must~~:~~

~~(a)~~ consider the circumstances and determine whether to make an internal notification of suspicious activity to the MLRO under Rule 14.2.2~~;~~ and then take the following steps:

(~~b~~a) where it has determined that it is unnecessary to make such a report, return to the customer any monies associated with the relationship or Transaction or ~~occasional transaction~~services, excluding any reasonable costs incurred by the Relevant Person; or

(~~c~~b) where it has determined that it is necessary to make such a report, not return any monies or provide any investments to the customer, unless instructed to do so by the MLRO and otherwise act in accordance with instructions issued by the MLRO; and

(~~d~~c) not establish any further business relationship with that customer until the verification process has been completed for that customer in accordance with these Rules.

~~8.2.2~~ ~~(1)~~8.2.3A Relevant Person must ensure that its AML/TFS systems and controls referred to in Rule ~~6.2.1~~4.1.1 include risk management policies and procedures concerning the conditions under which business relationships may be established ~~with a customer~~, or Transactions or services carried out, before completing verification of the identity of a customer and Beneficial Owners.

Guidance

1. Examples of situations that might lead a Relevant Person to have doubts about the veracity or adequacy of documents, data or information previously obtained might be where: there is a suspicion of money laundering in relation to that customer; there is a material change in the way that the customer's account is operated which is not consistent with the customer's business profile; or it appears to the Relevant Person that a Person other than the nominal customer is the real customer.

2. Situations that the Relevant Person may take into account include, for example, accepting subscription monies during a short offer period or executing a time

critical Transaction which, if not executed immediately, would or may cause a customer to incur a financial loss due to price movement or loss of opportunity or when a customer seeks immediate insurance cover.

3. When complying with Rule 8.2.1, a Relevant Person should also, where relevant, consider Rule 8.7.1 regarding failure to conduct or complete CDD and Chapter 14 regarding Suspicious Activity/Transaction Reports and tipping off.

8.3 Standard Customer Due Diligence requirements

8.3.1 (1) In undertaking Standard CDD a Relevant Person must:

...

(4) If a PEP is identified under (3), then the Relevant Person must, in addition to Standard CDD under 8.3.1, undertake Enhanced CDD under 8.4.1.

8.3.2 (1) For the purposes of Rule 8.3.1(1)(a), a Relevant Person must identify a customer and verify the customer's identity in accordance with this Rule.

(2) If a customer is a Natural Person, a Relevant Person must obtain and verify information about the person's:

(a) full name (including any alias);

(b) date and place of birth;

(c) nationality;

(d) legal domicile; ~~and~~

(e) current residential address, other than a post office box~~.~~; and

(f) where applicable, the name and address of the person's employer.

(3) If a customer is a Body Corporate, the Relevant Person must obtain and verify:

(a) the full name of the Body Corporate and any trading name and its legal form;

(b) the address of its registered office and, if different, its principal place of business;

(c) the date and place of incorporation or registration;

(d) ~~relevant corporate~~a copy of the certificate of incorporation or registration, and the articles of association or equivalent governing documents of the ~~customer~~Body Corporate; ~~and~~

(f) the company registration number, tax registration number (if any) and unique identification number (if any);

(e) the full names of the members of its Governing Body and persons exercising a ~~senior management~~Senior Management position~~.~~; and

(f) if the Body Corporate is constituted under the laws of a country other than the UAE, the name and address of its legal representative in the UAE (if any) together with supporting evidence.

...

Guidance ~~on CDD~~

1. The information required under 8.3.2(2)(a) and (b) should be obtained through a review of an original current, valid passport or, where a customer does not own a passport, an official identification document which includes a photograph. For the purposes of Rule 8.3.2(2)(a) and (b) an official government identification document in digital form and issued by a governmental competent authority is considered valid.

2. A Relevant Person should ensure that any documents used for the purpose of identification are original documents, whichever format they are in, including digital.

3. The verification of a customer's identity, including their address, should be based on official documents. Where that is not possible, a Relevant Person should consider using additional documents, data or information obtained from different reliable and independent sources to verify identity. Any lack of official documents and alternative means of verification should lead the Relevant Person to ~~re-assess~~reassess the customer's risk classification and the associated level of due diligence to be undertaken.

...

10. In undertaking CDD, a Relevant Person that is a Recognised Body should have regard to the provisions of the Market Infrastructure Rulebook ("**MIR**") requiring appropriate measures to be taken to prevent money laundering, Market Abuse and Financial Crime, including those set out at MIR 2.8.5(c) and MIR 2.9.

11. As set out in Chapter 4 and referenced in Chapter 7, a Relevant Person should maintain up-to-date lists of Jurisdictions Under Increased Monitoring and Jurisdictions Subject to a Call for Action, and screen against them as part of a customer risk assessment and CDD.

8.3.3 (1) For the purposes of Rule 8.3.1(1)(b), and subject to (4), a Relevant Person must identify the Beneficial Owners of a Body Corporate in accordance with this Rule.

...

(4) If no Natural Person can be identified pursuant to (2) and (3), a Relevant Person must treat the relevant Natural Person(s) holding a Senior Management position as the Beneficial Owner(s).

(~~4~~5) A Relevant Person is not required to comply with Rule 8.3.1(1)(b) if the customer is:

(a) a Listed Body Corporate; or

(b) a Body Corporate that is wholly-owned by the Federal Government of the UAE, or by any of the governments of the member Emirates of the UAE; or

(c) a Body Corporate created by Emiri decree within the UAE.

...

8.3.5 (1) For the purposes of Rule 8.3.1(1)(b), a Relevant Person must identify the Beneficial Owners of a customer that is a trustee of a trust or an equivalent position in respect of a similar Legal Arrangement in accordance with this Rule.

...

(3) For the purposes of (2)(e) "control" means a power, whether exercisable alone, jointly with another person or with the consent of another person, under the trust instrument or by law to:

(a) dispose of, advance, lend, invest, pay or apply trust property;

(b) vary or terminate the trust;

(c) add or remove a person as a beneficiary to or from a class of beneficiaries;

(d) appoint or remove trustees or give another person control over the trust; and

(e) direct, withhold consent to or veto the exercise of a power mentioned in ~~sub-paragraphs~~ (a) to (d).

(4) Where any of the persons identified under (2)(a) to (e) are fulfilled by a Body Corporate or Partnership, the Relevant Person must identify the Beneficial Owners of Body Corporate or Partnership in accordance with Rule 8.3.3 and Rule 8.3.4.

8.3.6 (1) For the purposes of Rule 8.3.1(1)(b), a Relevant Person must identify the Beneficial Owners of a customer that is a foundation or other Legal Arrangement similar to a foundation in accordance with this Rule.

..

Guidance ~~on verification of the identity of Beneficial Owners~~

1. In determining whether an individual meets the definition of Beneficial Owners, regard should be had to all the circumstances of the case, in particular the size of an individual's legal engagement or beneficial ownership in a Transaction.

...

4. A Relevant Person should take into account its obligations pursuant to Federal AML Legislation to obtain adequate information to identify Beneficial Owners. This includes each Beneficial Owner's full name, nationality, date and place of birth,

residential address, identity number and type, tax registration number (where applicable) and any other relevant information.

5. The relevant Natural Person(s) holding a Senior Management position for Rule 8.3.3(4) will usually be the individual(s) who hold the position of senior managing official of the Body Corporate.

~~**Guidance on Politically Exposed Persons (PEPs) and corruption**~~

~~1. Individuals who have, or have had, a high political profile, or hold, or have held, public office, may pose a higher money laundering risks to a Relevant Person as their position may make them prone to corruption. This risk also extends to members of their families and to known close associates. Being a PEP does not, in itself, of course, incriminate individuals or entities.~~

~~2. Generally, a foreign PEP presents a higher risk of money laundering because there is a greater risk that such a Person, if he were undertaking money laundering, would attempt to place his money offshore, away from his home jurisdiction, where he is less likely to be recognised as a PEP and where it would be more difficult for law enforcement agencies in his home jurisdiction to confiscate or freeze his criminal proceeds.~~

~~3. A Relevant Person should be aware that customer relationships with family members or close associates of PEPs involve similar risks to those with PEPs themselves.~~

~~4. The risk of corruption-related money laundering increases where a Relevant Person deals with a PEP. Corruption may involve serious crimes and has become the subject of increasing global concern. Corruption offences are predicate crimes under Federal AML Legislation.~~

~~5. The Regulator considers that after leaving office a PEP remains a higher risk for money laundering if such an individual continues to exert political influence or otherwise poses a risk of being involved in corruption.~~

~~6. The fact that an individual is a PEP does not automatically mean that the individual must be assessed to be a high-risk customer: however, Enhanced CDD still needs to be undertaken on PEPs. A Relevant Person will need to assess the particular circumstances relating to each PEP to determine what risk category is appropriate.~~

~~**Guidance on FATF Jurisdictions Under Increased Monitoring / Subject to a Call for Action**~~

~~1. A Relevant Person should maintain up-to-date lists of Jurisdictions Under Increased Monitoring and Jurisdictions Subject to a Call for Action and screen against them for potential exposure as part of CDD. Customer exposure to jurisdictions appearing on these lists should be taken into account when developing and applying risk-based measures relating to CDD. Customers exposed to such jurisdictions may present higher money laundering risks and specific counter-measures including Enhanced CDD may be required.~~

8.4 Enhanced Customer Due Diligence

8.4.1 ~~Where a~~A Relevant Person ~~is required to~~must undertake Enhanced CDD~~, having~~ on a customer assigned a ~~customer a~~ high-risk rating ~~or it or its Beneficial Owners is a PEP, then,~~ in addition to CDD under Rule 8.3.1, ~~it must~~as follows:

(a) obtain:

(i) additional identification information on the customer and all Beneficial Owners;

(ii) additional information on the intended nature of the business relationship;

(iii) information on the reasons for a Transaction;

...

(e) obtain the approval of Senior Management to commence or continue a business relationship with the customer; and

(f) require the first payment to be carried out through an account in the customer's name with a financial institution that is subject to AML/TFS regulation and supervision in a jurisdiction that has standards equivalent to those set out in the FATF Recommendations~~; and~~.

~~(g) for a customer who is a Natural Person, verify the current residential address (other than a post office box).~~

Guidance

1. In Rule 8.4.1, Enhanced CDD measures are mandatory to the extent that they are applicable to the relevant customer or the circumstances of the business relationship and to the extent that the risks would reasonably require it. Therefore, the extent of additional measures to be conducted is a matter for the Relevant Person to determine on a case-by-case basis.

2. In Rule 8.4.1(e), Senior Management approval may be given by an individual ~~member of the Relevant Person's Senior Management~~ or by a committee ~~of senior managers~~ appointed to consider high-risk customers that includes Senior Management. Such approval may also be outsourced within the Group, but only to a suitably qualified individual or committee.

...

8. A Relevant Person may commission a report from a third-party vendor to obtain further information on a customer or Transaction or to investigate a customer or Beneficial Owners in very high-risk cases. Such a report may be particularly useful where there is little or no publicly available information on a Person or on a Legal Arrangement or where the Relevant Person has difficulty in obtaining and verifying information.

Guidance on Politically Exposed Persons (PEPs) and corruption

1. Individuals who have, or have had, a high political profile, or hold, or have held, public office, may pose a higher money laundering risk to a Relevant Person as their position may create more risk of corruption.

2. This risk extends to family members and known close associates, and dealing with family members or close associates involves risks similar to those associated with PEPs themselves. The Regulator expects Relevant Persons to take a risk-based approach in assessing whether a person is a family member or close associate. A family member includes spouses or partners, children and their spouses/partners, parents and siblings. A close associate includes individuals who share beneficial ownership of a Legal Person or Legal Arrangement, hold beneficial ownership of a Legal Person or Legal Arrangement for their benefit or have a close professional, business or social relationship with the PEP.

3. Generally, a foreign PEP presents a higher risk of money laundering because there is a greater risk that such a Person would seek to move their money away from their home jurisdiction. Corruption offences are predicate crimes under Federal AML Legislation.

4. The Regulator considers that a PEP remains a higher risk for money laundering after leaving office, particularly if such an individual continues to exert political influence or otherwise poses a risk of being involved in corruption.

~~9. For Rule 8.4.1, circumstances where it may be applicable to require the first payment made by a customer in order to open an account with a Relevant Person to be carried out through a bank account in the customer's name include:~~

~~i. (a) where, following the use of other Enhanced Customer Due Diligence measures, the Relevant Person is not satisfied with the results of that due diligence; or~~

~~ii. (b) as an alternative measure, where one of the measures in Rule 8.4.1(a) to (e) cannot be carried out.~~

~~10. A Relevant Person should maintain up-to-date lists of Jurisdictions Under Increased Monitoring and Jurisdictions Subject to a Call for Action and take these lists into account in developing and applying risk-based measures relating to CDD including the development of compliance procedures.~~

~~11. CDD should include screening for customer exposure to Jurisdictions Under Increased Monitoring and Jurisdictions Subject to a Call for Action. Customer exposure to such jurisdictions may present higher money laundering risks and specific risk-based countermeasures may be required. In the case of customer exposure to Jurisdictions Under Increased Monitoring, this may include undertaking Enhanced CDD. In the case of customer exposure to Jurisdictions Subject to a Call for Action, Enhanced CDD should always be undertaken.~~

~~12. Pursuant to directives of the NAMLCFTC, Relevant Persons must exercise appropriate levels of due diligence on Transactions originating from, routed through or destined for Jurisdictions Subject to a Call for Action and any other~~

~~financial or non-financial engagement involving an individual or entity from such jurisdictions.~~

~~13. Relevant Persons should ensure they are aware of and comply with the requirements of the FIU relating to the filing of a High Risk Country Transaction Report or a High Risk Country Activity Report (as applicable) via goAML. Currently, these must be filed prior to conducting Transactions where the remitter or the beneficiary is an individual or entity associated with a Jurisdiction Subject to a Call for Action. Such Transactions may only be executed in line with guidance issued by the FIU.~~

...

8.6.1 When undertaking ongoing CDD under Rule 8.3.1(1)(d), a Relevant Person must:

(a) monitor Transactions undertaken during the course of its customer relationship to ensure that the Transactions are consistent with the Relevant Person's knowledge of the customer, ~~his~~their business and risk rating;

...

9. ~~AML/TFS COMPLIANCE AND THIRD PARTIES~~THIRD PARTY CDD, BUSINESS PARTNER DUE DILIGENCE AND OUTSOURCING ELEMENTS OF CDD

9.1 Reliance on a third ~~party~~party's CDD

9.1.1 (1) ~~A~~Subject to (2), a Relevant Person may rely on the following ~~third parties~~Persons to conduct one or more of the elements of CDD on its behalf:

(a) an Authorised Person or Recognised Body;

(b) a law firm, notary, or other independent legal business, accounting firm, audit firm or insolvency practitioner or an equivalent Person in another jurisdiction;

(c) a Financial Institution; or

(d) a member of the Relevant Person's Group~~; or~~.

~~ii. (e) other specialised utilities for the provision of outsourced AML/TFS services.~~

(2) Pursuant to Rule 4.9.4, a Relevant Person must not rely on a Person that is incorporated in or operating from a Jurisdiction Subject to a Call to Action to conduct one or more of the elements of CDD on its behalf.

(~~2~~3) In (1), a Relevant Person may rely on the information previously obtained by a third party which covers one or more elements of CDD.

(~~3~~4) Where a Relevant Person seeks to rely on a Person in (1)~~,~~ it may only do so if and to the extent that:

(a) it immediately obtains the necessary CDD information from the third party in (1);

(b) it takes adequate steps to satisfy itself that certified copies of the documents used to undertake the relevant elements of CDD will be available from the third party on request without delay;

(c) the Person in (1)(b) to (d) is~~ subject to regulation, including AML/TFS compliance requirements, by a Non-ADGM Financial Services Regulator or other competent authority in a country with AML/TFS regulations which are equivalent to the standards set out in the FATF Recommendations and it is supervised for compliance with such regulations;~~:

(i) subject to AML/TFS requirements that are equivalent to the standards set out in the FATF Recommendations; and

(ii) adequately supervised for compliance with those requirements by a competent authority;

(d) the Person in (1) has not relied on any exception from the requirement to conduct any relevant elements of CDD which the Relevant Person seeks to rely on; and

(e) in relation to (~~2~~3), the information is up to date.

(~~4~~5) Where a Relevant Person relies on a member of its Group~~ to conduct one or more of the elements of CDD on its behalf~~, such Group member need not meet the condition in (~~3~~4)(c) if:

~~iii.~~ ~~(a) the Group is subject to policies and requirements equivalent to FATF standards, either:~~

(~~i~~a) ~~where~~ the Group applies and implements ~~a~~ Group-wide ~~policy on CDD and record-keeping which is equivalent to~~policies on AML/TFS compliance that meet the standards set ~~by~~out in the FATF Recommendations; ~~or~~and

(~~ii~~b) ~~where the effective implementation of those CDD and record-keeping requirements and AML/TFS programmes are supervised at Group level~~the Group is supervised for compliance with those policies by a Non-ADGM Financial Services Regulator ~~or other competent authority in a jurisdiction~~in a country with AML/TFS ~~regulations that are~~requirements equivalent to the standards set out in the FATF Recommendations~~;~~.

~~iv.~~ ~~(b) no exception from identification obligations has been applied in the original identification process; and~~

~~v.~~ ~~(c) a written statement is received from the introducing member of the Relevant Person's Group confirming that:~~

~~(i) the customer has been identified in accordance with the relevant standards under (4)(a) and (b);~~

~~(ii) any identification evidence can be accessed by the Relevant Person without delay; and~~

~~(iii) the identification evidence will be kept for at least six years.~~

(~~5~~6) If a Relevant Person is not reasonably satisfied that a customer or Beneficial ~~Owners~~Owner has been identified and verified by a third party in a manner consistent with these Rules, the Relevant Person must immediately perform the CDD itself with respect to any deficiencies identified.

(~~6~~7) Notwithstanding the Relevant Person's reliance on a Person in 9.1.1(1), the Relevant Person remains responsible for compliance with, and liable for any failure to meet the CDD requirements ~~in the AML Rulebook~~of, Anti-Money Laundering Legislation.

9.1.2 (1) When assessing under Rule 9.1.1(~~3) or (~~4) or (5) if AML/TFS ~~regulations~~requirements in another jurisdiction are equivalent to ~~FATF~~the standards set out in the FATF Recommendations, a Relevant Person must take into account factors including~~, but not limited to~~:

(a) mutual evaluations, assessment reports or follow-up reports published by FATF, the IMF, the World Bank, the OECD or other International Organisations;

(b) membership of FATF or other international or regional groups such as the MENAFATF or the Gulf Co-operation Council;

(c) contextual factors such as political stability or the level of corruption in the jurisdiction;

(d) evidence of recent criticism of the jurisdiction, including in:

(i) FATF advisory notices;

(ii) public assessments of the jurisdiction's AML/TFS regimes by organisations referred to in (a); or

(iii) reports by other relevant non-government organisations or specialist commercial organisations;

(e) whether adequate arrangements exist for co-operation between the competent authority for AML/TFS ~~regulator~~compliance in that jurisdiction and the Regulator.

(2) A Relevant Person making an assessment under (1) must rely only on sources of information that are reliable and up to date.

(3) A Relevant Person must keep adequate records of how it made its assessment, including the sources and materials considered.

Guidance

1. In complying with Rule 9.1.1(~~3~~4)(a), "immediately obtaining the necessary CDD information" means obtaining all relevant CDD information, and not just basic information such as name and address. ~~However, compliance~~Compliance can be achieved by ~~having~~sending the information ~~sent in an~~via email or ~~other~~another appropriate means. ~~For the avoidance of doubt, it does not necessarily require a~~A Relevant Person is not required to immediately obtain the underlying certified documents used by the third party to undertake its CDD ~~because under~~. However, pursuant to Rule 9.1.1(~~3~~4)(b), these ~~need only~~must be available on request without delay.

2. The Regulator would expect a Relevant Person, in complying with Rule 9.1.1(~~5~~6), to fill any gaps in the CDD process as soon as it becomes aware that a customer or Beneficial Owners has not been identified and verified by the third party in a manner consistent with these Rules.

3. If a Relevant Person acquires another business, either in whole or in substantial part, the Regulator would permit the Relevant Person to rely on the CDD conducted by the business it is acquiring, but would expect the Relevant Person to have done the following:

   (a) as part of its due diligence for the acquisition, to have taken a reasonable sample of the prospective customers to assess the quality of the CDD undertaken; and

   (b) to have undertaken CDD on all the customers to cover any deficiencies identified in (a) as soon as possible following the acquisition, prioritising high-risk customers.

4. Where the legislative framework of a jurisdiction (such as secrecy or data protection legislation) prevents a Relevant Person from having access to CDD information upon request without delay as referred to in Rule 9.1.1(~~3~~4)(b), the Relevant Person should undertake the relevant CDD itself and should not seek to rely on the relevant third party.

~~5. If a Relevant Person relies on a third party located in a foreign jurisdiction to conduct one or more elements of CDD on its behalf, the Relevant Person must ensure that the foreign jurisdiction has AML/TFS regulations which are equivalent to the standards in the FATF Recommendations (see Rule 9.1.1(3)(c)).~~

~~6. Relevant Persons should follow directives issued by the NAMLCFTC. For example, Relevant Persons are prohibited from using third parties located in Jurisdictions Subject to a Call for Action to perform CDD.~~

5. Where an Authorised Person is providing a Client Money account for another Financial Institution, the Regulator expects that:

   (a) the Financial Institution remains responsible for undertaking CDD and ensuring compliance with other requirements of the AML Rulebook or equivalent legislation applicable to it;

(b) the Authorised Person should undertake a risk assessment and appropriate CDD on the Financial Institution, including understanding the nature of the Financial Institution's business and the types of customers that the Financial Institution has; and

(c) notwithstanding the Financial Institution's obligation to undertake CDD on its own clients, the Authorised Person should still undertake Sanctions screening and transaction monitoring for all payments made via its systems.

9.2 ~~Business~~Know your business partner ~~identification~~

9.2.1 ~~(1)~~ Prior to establishing the business relationship, a Relevant Person must establish and verify the identity of its business partners by obtaining sufficient and satisfactory evidence of the identity of any business partner it relies upon in carrying on its Regulated Activities.

~~(a)~~9.2.2 A Relevant Person must maintain accurate and up-to-date information and conduct ongoing due diligence on its business partners~~,~~ throughout the course of the business relationship.

~~(b)~~9.2.3 If at any time a Relevant Person becomes aware that it lacks sufficient information or documentation concerning a business partner's identification, or develops a concern about the accuracy of its current information or documentation, it must promptly obtain appropriate material to verify such business partner's identity.

Guidance

~~(2) In the context of this Rule, a~~

1. A 'business partner' includes:

~~(a).~~ ~~a third party as~~any of the Persons specified in Rule 9.1.1(1);

~~(b).~~ a ~~member of the~~service provider performing elements of CDD for a Relevant ~~Person's Group~~Provider, pursuant to Rule 9.3.1; and

~~(c).~~ ~~a Correspondent Bank; or~~ other service providers.

~~vi. (d) any other service provider.~~

~~3. (3) A Relevant Person that establishes, operates or maintains a Correspondent Account for a Correspondent Banking Client must ensure that it has arrangements to:~~

~~i. (a) conduct due diligence in respect of the opening of a Correspondent Account for a Correspondent Banking Client, including measures to identify:~~

~~(i) its ownership and management structure;~~

(ii) its major business activities and customer base;

(iii) its location; and

(iv) the intended purpose of the Correspondent Account;

ii. (b) identify all third parties that will use the Correspondent Account; and

iii. (c) monitor Transactions processed through a Correspondent Account that has been opened by a Correspondent Banking Client, in order to detect and report any suspicion of money laundering.

Guidance

Under (2)(d), serviceService providers include agents that directly facilitate the activities of AuthorisedRelevant Persons in servicing their clients, as distinct from other service providers that provide purely ancillary services, such as IT,software or facilities management etc. to an Authorised, where the money laundering risks of the relationship to a Relevant Person are low.

9.2.2 A Relevant Person must not:

4. (1) establish a correspondent banking relationship with a Shell Bank;

5. (2) establish or keep anonymous accounts or accounts in false names; or

6. (3) maintain a nominee account which is held in the name of one Person, but controlled by or held for the benefit of another Person whose identity has not been disclosed to the Relevant Person.

Guidance

1. "Know your business partner" is as important as "Know Your Customer". A Relevant Person is therefore required to verify the identity of a prospective business partner and to obtain evidence of it. The same documentation that is used to identify customers should be obtained from the business partner prior to conducting any business.

2. A Relevant Person should verify whether any secrecy or data protection law exists in the country of incorporation of the business partner that would prevent access to relevant data, and if necessary, comply with Rule 4.5.6.

3. The requirement to identify the business partner is meant to cover only those business partners who may pose any relevant money laundering risks to the Relevant Person. Hence, a Relevant Person would not be required to establish and verify the identity of, for example, its maintenance or cleaning service.

4. The Regulator may take into account the identity of a Relevant Person's business partner and the nature of their relationship in considering the fitness and propriety of a Relevant Person.

~~5. Before entering into a business relationship, a Relevant Person should conduct a due diligence investigation, which includes ensuring that the business partner is an existing Person authorised to conduct the kind of business in question and, if applicable, verifying that this Person is duly regulated by a Financial Services Regulator or other relevant regulatory authority or regulator. In accordance with "The Wolfsberg Anti-Money Laundering Principles for Correspondent Banking", the Relevant Person should take into account, and verify the nature of:~~

~~i. (a) the business to be conducted and the major business activities of the business partner;~~

~~ii. (b) the jurisdiction where the business partner is located as well as that of its parent; and~~

~~iii. (c) the transparency and the nature of the ownership and the management structure.~~

~~6. A Relevant Person may also gather information about the reputation of the business partner, including whether it has been subject to investigation or regulatory action in relation to money laundering.~~

~~7~~3. A Relevant Person should adopt a risk-based approach when verifying its business partners' identities. Depending on the money laundering ~~risks~~risk assessment of the Relevant Person's business partner, the Relevant Person should ~~decide~~determine the level of detail ~~of~~for the business partner identification and verification process.

~~8~~4. A Relevant Person should have in place specific arrangements to ensure that adequate due diligence and identification measures with regard to the business relationship are taken.

~~9~~5. The Relevant Person should conduct regular reviews of the relationship with its business partners.

6. The same documentation that is used to identify customers should be obtained from the business partner before conducting any business.

7. The Regulator may take into account the identity of a Relevant Person's business partner(s) and the nature of their relationship in considering the fitness and propriety of a Relevant Person.

~~10. The Senior Management or Governing Body of a Relevant Person should give its approval before it establishes any new correspondent banking relationships.~~

~~11. A Relevant Person should also have arrangements to guard against establishing a business relationship with business partners who permit their accounts to be used by Shell Banks; further details on the definition of Shell Banks are set out in Guidance 2 to Rule 10.2.2.~~

9.3 Outsourcing ~~and agents~~elements of CDD

9.3.1 A Relevant Person which outsources any ~~one or more elements~~element of its CDD to a service provider~~(~~, including ~~those~~a service provider within its Group~~)~~, remains responsible for compliance with, and liable for any failure to meet~~, such obligations~~ the requirements of, Anti-Money Laundering Legislation.

~~**9.3.1A** Prior to appointing a service provider to undertake CDD, a Relevant Person must undertake an initial assurance assessment to evaluate the suitability of the service provider and must ensure that the service provider's obligations are clearly documented in a binding agreement.~~

9.3.2 A Relevant Person must not outsource any element of its CDD to a service provider incorporated in or operating from a Jurisdiction Subject to a Call to Action.

9.3.3 Before appointing a service provider to undertake any element of CDD, a Relevant Person must:

(1) evaluate the suitability of the service provider;

(2) establish that the services are reliable;

(3) assess whether the service provided will ensure the Relevant Person remains compliant with applicable legislation, including Anti-Money Laundering Legislation; and

(4) clearly document the services to be provided in a binding agreement.

~~**9.3.1B**~~9.3.4 After engaging a service provider~~the,~~ a Relevant Person must undertake periodic assurance assessments to ensure that the services ~~provided meet the obligations recorded in the binding~~comply with the agreement and allow ~~it to meet all the requirements that it is subject to~~the Relevant Person to remain in compliance with Anti-Money Laundering Legislation.

Guidance

1. An Authorised Person is also required to comply with the outsourcing obligations in GEN Rules 3.3.31 and 3.3.32 and PRU 6.8. A Recognised Body is also required to comply with the outsourcing obligations in MIR 2.14.

~~1~~2. ~~The use by a Relevant Person of~~Outsourcing elements of CDD includes using digital identity verification services, screening services and using a service provider's eKYC System ~~that enables a Relevant Person to undertake eKYC constitutes outsourcing for the purposes of Rule 9.3.1~~for Section 9.3.

~~2~~3. When undertaking an ~~assurance~~ assessment of an eKYC System for ~~the purpose of Rule 9.3.1A, a Relevant Person should seek to establish that the eKYC System is reliable and independent, and allows the Relevant Person to comply with all applicable legislation including applicable Rules and Regulations. In addition~~Rule 9.3.3(3), a Relevant Person should consider ~~applying guidance on~~relevant

assurance standards issued by ~~the Regulator,~~ competent ~~UAE~~ authorities~~, FATF, and other relevant standard setting~~ and standard-setting bodies.

~~3. In limited circumstances, a Relevant Person may place reliance on the assurance assessment of the eKYC System conducted entirely by another entity. Such circumstances comprise the following.~~

~~iv. (a) Where an assurance assessment of the eKYC System has been undertaken by a Related entity and specifically addresses the legislation applicable to the Relevant Person. In such circumstances, the Relevant Person remains responsible for the eKYC System's compliance with applicable legislation including applicable Rules and Regulations and it should maintain a copy of the assessment.~~

4. Where a Relevant Person relies on a third party (including a member of its Group) to undertake an assessment of an eKYC System on its behalf for Rule 9.3.3, the Relevant Person should:

(a) ensure the third party is competent and independent, with relevant expertise and resources;

(b) receive and maintain a copy of the assessment; and

(c) ensure the assessment specifically addresses the requirements of the service necessary to ensure the Relevant Person remains compliant with applicable legislation including Anti-Money Laundering Legislation.

~~(b)~~5. Where the eKYC System has been authorised or approved by a competent authority of the UAE or a competent authority in a jurisdiction with AML/TFS laws equivalent to the UAE ~~In such circumstances, the eKYC system should be authorised for use in CDD. Further, the Relevant Person should~~, a Relevant Person may take such authorisation or approval into account in assessing the suitability of the eKYC System, but should still undertake its own review ~~to ensure that any use of the relevant eKYC System is appropriate and enables compliance with all legislation applicable to the Relevant Person including applicable Rules and Regulations~~.

~~v. (c) Where a Relevant Person chooses to employ a third party to assist in its own assurance assessment of the eKYC System, it should ensure that a competent and independent firm with relevant expertise and resources be employed. The Relevant Person remains wholly responsible for the eKYC System's compliance with, and any failure to meet, the legislation applicable to the Relevant Person including applicable Rules and Regulations.~~

~~4~~6. ~~In complying with Rule 9.3.1, a~~A Relevant Person should ensure that the service provider can be replaced with minimal disruption ~~in the event~~if the outsourcing arrangement is terminated.

~~5. An Authorised Person is also required to comply with the outsourcing obligations in GEN 3.3.31 and 3.3.32 and PRU 6.8. A Recognised Body is also required to comply with the outsourcing obligations in MIR 2.14.~~

~~9.2.2~~9.3.5 Authorised Persons Providing Money Services

(1) An Authorised Person that is engaged in Providing Money Services must:

(~~b~~a) maintain a complete, current and accurate register of all agents and members of its Group it uses to conduct its operations and make that register available to the Regulator upon request;

(~~c~~b) include all agents and members of its Group identified in (a) as part of its AML/TFS compliance programme and monitor the compliance of such agents and members of its Group with the requirements of its AML/TFS programme;

(~~d~~c) comply with all AML/TFS requirements imposed in all jurisdictions within which it operates and ensure the compliance of its agents and members of its Group operating on its behalf with all AML/TFS requirements in the jurisdictions in which they are operating;

(~~e~~d) when executing a Payment Transaction, assess and consider all relevant information, including information about the Payer and the Payee, including any beneficiary as may be applicable, and require its agents and members of its Group, as appropriate, to determine whether a Suspicious Activity/Transaction Report should be filed by it or its agents or a member of its Group; and

(~~f~~e) where appropriate, ensure that the relevant equivalent of a Suspicious Activity/Transaction Report is filed in all other jurisdictions related to a suspicious Payment Transaction and make available to all authorities responsible for AML/TFS compliance all transaction information related to the suspicious transaction.

(2) An Authorised Person making an assessment under (1) must rely upon current sources of information when making such assessment and must keep adequate records concerning such assessments, including all sources and materials considered, for a period of at least six years.

Guidance

1. Agents directly facilitate the activities of Authorised Persons in servicing their clients, as distinct from other service providers that provide purely ancillary services, such as IT, facilities management, etc., to an Authorised Person.

2. Payment Service Providers should be aware of the prohibition in COBS Rule 19.7.1 in relation to accepting and distributing physical cash to and from Payment Service Users.

10. CORRESPONDENT BANKING, ~~WIRE~~ELECTRONIC FUND TRANSFERS, VIRTUAL ASSETS AND FIAT-REFERENCED TOKENS TRANSFERS AND THE TRAVEL RULE, AUDIT AND ANONYMOUS ACCOUNTS ~~AND AUDIT~~

10.1 ~~Application~~Correspondent Banking

~~**10.1.1** This Chapter applies to Recognised Bodies and all Authorised Persons, other than Credit Rating Agencies and Representative Offices.~~

~~10.2 Correspondent banking~~

~~**10.2.1**~~10.1.1 An Authorised Person proposing to ~~have a correspondent banking~~enter into a Correspondent Banking relationship ~~with a respondent bank~~ must:

(a) undertake appropriate CDD on the ~~respondent bank~~Respondent Bank;

(b) as part of (a), gather sufficient information about the ~~respondent bank to understand~~Respondent Bank to fully understand the nature of ~~the~~its business, including making appropriate enquiries as to its ownership and management, its major business activities and customer base, the countries or jurisdictions in which it operates and the intended purpose of the Correspondent Account;

(c) determine from publicly available information the reputation of the ~~respondent bank~~Respondent Bank and the quality of supervision that is subject to, including whether it has been the subject of a money laundering investigation or relevant regulatory action;

(d) assess the ~~respondent bank's~~Respondent Bank's AML/TFS controls and ascertain ~~if~~where they are adequate and effective in light of the FATF Recommendations;

(e) ~~ensure that~~obtain prior approval ~~of the Authorised Person's~~from Senior Management ~~is obtained before entering into a new correspondent banking~~before establishing the Correspondent Banking relationship;

(f) ensure that the respective responsibilities of the ~~parties to the correspondent banking relationship are~~Correspondent Bank and Respondent Bank are clearly understood and properly documented;

(g) be satisfied that, in ~~respect of~~relation to any customers of the ~~respondent bank who~~Respondent Bank that will have direct access to ~~accounts of the Authorised Person, the respondent bank~~the Correspondent Bank Account(s), the Respondent Bank:

(i) has undertaken CDD (including ongoing CDD) at least equivalent to that in Rule 8.3.1 in respect of each customer; and

(ii) is able to provide the relevant CDD information in (i) to the ~~Authorised~~

~~Person~~Correspondent Bank upon request; and

(h) document the basis for its satisfaction that the requirements in (a) to (g) are met.

~~10.2.2~~10.1.2 An Authorised Person must:

(a) not enter into a ~~correspondent banking~~Correspondent Banking relationship with a Shell Bank or with any Financial Institution that permits a Shell Bank to use its account(s); and

(b) take appropriate measures to ensure that it does not enter into, or continue a ~~corresponding~~correspondent banking relationship with, a ~~bank~~Financial Institution which is known to permit its accounts to be used by Shell Banks.

10.1.3 An Authorised Person must ensure that it has arrangements to:

(a) undertake ongoing monitoring of any Correspondent Banking relationship and any Respondent Banks;

(b) identify on an ongoing basis all third parties that will use the Correspondent Account; and

(c) monitor on an ongoing basis the Correspondent Account and all transactions processed through the Correspondent Account, in order to detect and report any suspicion of money laundering.

Guidance

1. Correspondent Banks should review and take into account industry best practice including the Wolfsberg Group's "Financial Crime Principles for Correspondent Banking" and guidance issued by the FATF in relation to Correspondent Banking relationships.

~~1. The rules and guidance set out in Rule 9.2 above also apply to correspondent banking business partners. This Rule provides further details on specific requirements applicable to a correspondent banking business relationship.~~

~~2. With regard to Correspondent Banking Clients and, if applicable, other qualified professionals, specific care should be taken to assess their AML/TFS arrangements regarding customer identification, Transaction monitoring, terrorist financing and other relevant elements, and to verify that these business partners comply with the same or equivalent AML/TFS requirements as the Relevant Person. Information on applicable laws and regulations regarding the prevention of money laundering should be obtained.~~

~~3. A Relevant Person should ensure that a Correspondent Banking Client does not use the Relevant Person's products and services to engage in business with Shell Banks. A Shell Bank would be a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial Group that is subject to effective consolidated supervision. The Regulator does not consider that the existence of a local agent or low-level staff constitutes physical presence.~~

~~4~~2. ~~If applicable~~Where necessary, information on a Respondent Bank's distribution networks and delegation of duties should be obtained by the Correspondent Bank.

3. An Authorised Person or Recognised Body should take into account the requirements of Article 26 of the AML Regulations in relation to Correspondent Banking.

~~10.3~~ ~~Wire~~10.2 Electronic fund transfers and the ~~Travel Rule~~travel rule

~~10.3.1~~ ~~In this section:~~

~~(a) "**account**" includes a digital wallet when the wire transfer is a transfer of Virtual Assets;~~

10.2.1 Application

(1) This section 10.2 does not apply to:

(a) an Authorised Person or Recognised Body that provides Financial Institutions with messages or other support systems for fund transfers;

(b) ~~"**account holder**" includes a wallet holder when the wire transfer is a transfer of Virtual Assets;~~a transfer and settlement between Financial Institutions where both the originator and the beneficiary are Financial Institutions acting on their own behalf.

~~(c) "**account number**" includes a wallet address when the wire transfer is a transfer of Virtual Assets;~~

10.2.2 Definitions

(1) In this section 10.2:

(~~d~~a) "**batch transfer**" means a transfer comprised of ~~a number of~~multiple individual ~~wire~~fund transfers from a single originator that are bundled for transmission, whether or not the individual ~~wire~~fund transfers are ~~intended~~ ultimately intended for one or more beneficiaries;

(~~e~~b) "**beneficiary**" means the ~~Natural or Legal Person or the Legal Arrangement that is~~Person identified by the originator as the ~~receiver~~recipient of the requested ~~wire~~fund transfer;

(c) "**beneficiary institution**" means the Financial Institution that receives a fund transfer from the originating institution , whether directly or through an intermediary institution, and makes the funds available to a beneficiary;

(d) "**customer identification number**" means a number that is different from the unique transaction reference number and:

(i) uniquely identifies the originator to the originating institution; and

(ii) refers to a record held by the originating institution that contains at least one of the following: the originator's address, national identity number such as an identity card number or passport number, or date and place of birth;

(e) "**fund transfer**" means any electronic transfer of funds to a beneficiary on behalf of an originator through a Financial Institution, excluding transfers of Virtual Assets and Fiat-Referenced Tokens, and irrespective of whether the originator and the beneficiary are the same Person;

(f) "**intermediary institution**" means the Financial Institution in a payment chain that receives and transmits the fund transfer on behalf of the originating institution or the beneficiary institution or another intermediary institution;

(g) "**originating institution**" means the Financial Institution that the originator has instructed to make the fund transfer to the beneficiary;

(~~f~~h) "**originator**" means the account holder who instructs the ~~wire~~fund transfer from the relevant account, or where there is no account, the ~~Natural or Legal~~ Person that places the order with the ~~ordering Financial Institution~~originating institution to perform the ~~wire~~fund transfer; and

~~(g) "wire transfer" includes any value transfer arrangement.~~

(i) "**unique reference number**" means a unique reference number for the specific fund transfer that enables the relevant Financial Institutions to trace the fund transfer.

~~10.3.2~~10.2.3 (1) An Authorised Person ~~and~~or Recognised Body must:

(a) ~~when it sends or receives a wire transfer on behalf of a customer,~~ ensure that ~~the wire~~a fund transfer and any related messages contain ~~accurate originator and beneficiary~~the information required by (2) when sending or receiving a fund transfer;

(b) ensure that, while ~~the wire~~a fund transfer is under its control, the information ~~in (a)~~accompanying it remains with the ~~wire~~fund transfer and any related message throughout the payment chain;

(c) monitor ~~wire~~fund transfers for the ~~purpose~~purposes of detecting those ~~wire~~fund transfers that do not contain both originator and beneficiary information and enabling it to take appropriate measures to identify and mitigate any money laundering risks; and

(d) not effect ~~wire~~or accept fund transfers without the information required under (~~3~~2) and (~~4~~3).

~~7. (2) The requirement in (1) does not apply to an Authorised Person or Recognised Body which:~~

~~(a) provides Financial Institutions with messages or other support systems for wire transfers; or~~

~~(b) undertakes a wire transfer to another Financial Institution where both the originator and the beneficiary are Financial Institutions acting on their own behalf.~~

(~~3~~2) An Authorised Person ~~and~~or Recognised Body must ensure that information accompanying all ~~wire~~fund transfers contains at a minimum:

(a) the full name of the originator;

(b) the originator account number where ~~such an~~that account is used to process the ~~Transaction~~fund transfer, or a unique ~~Transaction~~ reference number ~~if~~where no originator account number exists;

(c) any one of the following:

(i) the originator's address;
(ii) the originator's national identity number, such as an identity card number or passport number;
(iii) the originator's customer identification number; or
(~~c~~iv) the ~~originator's address, or national identity number, or travel document number, or customer identification number, or~~ date and place of birth of the originator;

(d) the full name of the beneficiary; and

(e) the beneficiary account number where such an account is used to process the ~~Transaction~~fund transfer or a unique ~~Transaction~~ reference number ~~if~~where no beneficiary account number exists.

(~~4~~3) ~~An~~Before effecting a fund transfer, an Authorised Person ~~and~~or Recognised Body that is an originating institution must ~~ensure that for batch transfers~~:

(a) ~~it has verified~~verify the originator information ~~required~~that will accompany the fund transfer under (~~3~~)~~(a) to (c~~2); ~~and~~

(b) ensure that for batch transfers, the batch file contains the ~~beneficiary~~ information ~~required under (3)(d) and (e) for each beneficiary~~set out in (2) and that the beneficiary information included is fully traceable in ~~the beneficiaries~~each beneficiary's jurisdiction~~.~~; and

(c) record adequate details of the fund transfer that are sufficient to enable its reconstruction, including but not limited to, the date of the transfer, the originator and beneficiary, the type and amount of funds transferred and the value date.

(4) An Authorised Person or Recognised Body that is a beneficiary institution must identify and verify the identity of the beneficiary where the identity has not been previously verified.

(5) An Authorised Person or Recognised Body that sends or receives fund transfers must ensure that its AML/TFS systems and controls referred to in Rule 4.1.1 include risk management policies and procedures specifying the steps to be taken where a fund transfer lacks information required under this section, including when to reject or amend a transfer and any follow-up action that is to be taken.

Guidance

~~1. 'FATF Recommendation Number 16' seeks to ensure that national or international electronic payment and message systems, including fund or wire transfer systems such as SWIFT, are not misused as a means to break the money laundering audit trail. Therefore, the information about a customer as the originator of the wire transfer should remain with the payment instruction throughout the payment chain.~~

~~2~~1. ~~Relevant~~Authorised Persons and Recognised Bodies should monitor for, and conduct enhanced scrutiny of, suspicious activities, including incoming ~~wire~~fund transfers that do not contain complete originator information~~, including name, address and account number or unique reference number~~.

~~3~~2. The Regulator considers that concealing or removing ~~in a wire transfer~~ any of the information required by Rule ~~10.3.2~~10.2.3(~~3~~2) in a fund transfer would be a breach of ~~the requirement to ensure that the wire transfer contains accurate originator and beneficiary information~~that Rule.

10.3 Transfers of Virtual Assets and Fiat-Referenced Tokens and the travel rule

10.3.1 Application

(1) Section 10.3 applies to all Authorised Persons and Recognised Bodies, subject to the following:

(a) it does not apply to an Authorised Person or Recognised Body that is only providing messages or other support systems for VA/FRT transfers;

(b) it does not apply to a VA/FRT transfer (as defined below) between Financial Institutions where both the originator and the beneficiary are Financial Institutions acting on their own behalf;

(c) Rule 10.3.4 applies to an Authorised Person or Recognised Body only when it is the originating institution of a VA/FRT transfer; and

(d) Rule 10.3.5 applies to an Authorised Person or Recognised Body only when it is the beneficiary institution of a VA/FRT transfer.

10.3.2 Definitions

In this section 10.3:

(a) "**account**" includes a digital wallet or any record of an interest in a Virtual Asset or Fiat-Referenced Token;

(b) "**account number**" means the account number used to process the relevant VA/FRT transfer, including a wallet address, or a unique reference number where no account number exists;

(c) "**batch transfer**" means a transfer comprised of multiple individual VA/FRT transfers from a single originator that are bundled for transmission, whether or not the individual VA/FRT transfers are ultimately intended for one or more beneficiaries;

(d) "**beneficiary**" means the Person identified by the originator as the recipient of the requested VA/FRT transfer;

(e) "**beneficiary institution**" means the Person that, in the course of business, receives the VA/FRT transfer from the originating institution, whether directly or indirectly, in order to make the Virtual Assets or Fiat-Referenced Tokens available to the beneficiary;

(f) "**cross-border transfer**" means a VA/FRT transfer that is not a domestic transfer;

(g) "**customer identification number**" means a number that is different from the unique transaction reference number and:

(i) uniquely identifies the originator to the originating institution; and

(ii) refers to a record held by the originating institution that contains at least one of the following: the originator's address, national identity number or date and place of birth;

(h) "**domestic transfer**" means a VA/FRT transfer where the originating institution and the beneficiary institution are in the UAE, notwithstanding that the system used to process the VA/FRT transfer may be located in another country;

(i) "**originating institution**" means the Person that, in the course of business, receives instructions from the originator to make the VA/FRT transfer to the beneficiary;

(j) "**originator**" means the Person on whose behalf a VA/FRT transfer is initiated, and includes the originating institution acting on its own behalf;

(k) "**relevant transfer information**" means, unless otherwise specified:

(i) the full name of the originator;

(ii) the originator account number;

(iii) the originator's residential or business address;

(iv) any one of the following:

A. the originator's national identity number, such as an identity card number or passport number;

B. the originator's customer identification number; or

C. the date and place of birth of the originator;

(v) the full name of the beneficiary; and

(vi) the beneficiary account number;

(l) "**unhosted wallet**" includes a non-custodial wallet or wallet address operated, held, maintained or controlled by an originator or beneficiary without the provision of any services to the originator or beneficiary by a third party other than the provision of technology that enables the originator or beneficiary to administer their own Virtual Assets or Fiat-Referenced Tokens or the related cryptographic keys;

(m) "**unique reference number**" means a unique reference number for the specific VA/FRT transfer that enables the relevant originating institution and beneficiary institution to trace the VA/FRT transfer; and

(n) "**VA/FRT transfer**" means:

(i) any transfer of Virtual Assets or Fiat-Referenced Tokens to a beneficiary on behalf of an originator through another Person, such Person acting in the course of business, irrespective of whether the originator and the beneficiary are the same person; or

(ii) any transfer of Virtual Assets or Fiat-Referenced Tokens to or from an unhosted wallet.

10.3.3 **Requirements for all Authorised Persons and Recognised Bodies**

(1) In relation to VA/FRT transfers, an Authorised Person or Recognised Body must:

(a) ensure that an accompanying or related message or payment instruction contains relevant transfer information;

(b) ensure that, while a VA/FRT transfer is under its control, all information accompanying or related to a VA/FRT transfer remains with the VA/FRT transfer and any related message throughout the payment chain; and

(c) monitor VA/FRT transfers in order to take appropriate measures to identify and mitigate any money laundering risks, including:

(i) identifying VA/FRT transfers that lack relevant transfer information and taking appropriate follow-up action;

(ii) tracking of the transaction history of Virtual Assets or Fiat-Referenced Tokens to accurately identify their source and destination; and

(iii) identification of VA/FRT transfers that may be associated with illicit or suspicious activities.

(2) An Authorised Person or Recognised Body that sends or receives VA/FRT transfers must:

(a) have adequate policies and procedures in place to mitigate the money laundering risks arising from VA/FRT transfers;

(b) undertake appropriate Counterparty due diligence; and

(c) retain a record of all information it collects, creates and receives pursuant to this section 10.3, including details of all VA/FRT transfers sufficient to enable their reconstruction.

(3) The policies and procedures in (2)(a) must, without limitation, address where:

(a) the Authorised Person or Recognised Body is the originating institution, and the beneficiary institution is unable to receive relevant transfer information, as contemplated by Rule 10.3.4(5);

(b) the Authorised Person or Recognised Body is the beneficiary institution, and the VA/FRT transfer is received without relevant transfer information, as contemplated by Rule 10.3.5(4);

(c) the Authorised Person or Recognised Body receives a VA/FRT transfer from an unhosted wallet without relevant transfer information, as contemplated by Rule 10.3.6(3);

(d) a VA/FRT transfer should be reported to the Regulator, or a SAR/STR should be filed; and

(e) any further follow-up action may need to be taken in connection with (a)-(d), including as a result of a response to reporting under (d).

Guidance

1. The Regulator considers that concealing or removing any information accompanying a VA/FRT transfer would be a breach of Rule 10.3.3(1)(b).

2. The policies and procedures put in place under 10.3.3(2)(a) should include, but not be limited to, the requirements set out in Rule 10.3.3(2)(b) and 10.3.3(1).

3. The Regulator considers that Authorised Persons and Recognised Bodies will act as the originating institution or the beneficiary institution in connection with a VA/FRT transfer and accordingly does not prescribe separate obligations for intermediary institutions.

4. The Regulator expects ~~compliance by~~ Authorised Persons and Recognised Bodies to be aware of and comply with 'FATF Recommendation ~~Number~~number 15', FATF's Interpretative Note (R.15/INR.15) and 'FATF Recommendation ~~Number~~number 16' ~~that include requirements to obtain, hold, and transmit originator and beneficiary information and to not allow transfers where such information is lacking including where the value transfer involves Virtual Assets. Authorised Persons and Recognised Bodies should note that, pursuant to section 10.3, the Regulator does not differentiate between the responsibilities of the originator or the beneficiary when it comes to ensuring that all relevant information accompanies a wire transfer, and that no de minimis threshold is applied to the size of a relevant wire transfer.~~.

5. Further to Chapter 14, in determining whether a SAR/STR should be filed in relation to a VA/FRT transfer, Authorised Persons and Recognised Bodies should take into account all relevant information relating to the sending and receiving of the transfer.

10.3.4 **Additional requirements for the originating institution**

(1) Before effecting a VA/FRT transfer, an Authorised Person or Recognised Body must:

(a) collect relevant transfer information and, subject to (2), verify that information; and

(b) conduct appropriate due diligence on the beneficiary institution and satisfy itself that the beneficiary institution is appropriately regulated in accordance with applicable laws in the jurisdiction(s) in which it is incorporated and located.

(2) An Authorised Person or Recognised Body is not required to verify relevant transfer information where the daily aggregated value of VA/FRT transfers for the originator is less than USD 1,000, and none of the transfers are suspicious transactions.

(3) For VA/FRT transfers processed as a batch transfer, an Authorised Person or Recognised Body must include the relevant transfer information in the batch file, verify that information as required by Rule 10.3.4(1)(a), and ensure that the information included for each beneficiary is traceable in that beneficiary's jurisdiction.

(4) For domestic transfers where the relevant transfer information is available to the beneficiary institution by other means, an Authorised Person or Recognised Body may effect a domestic transfer with an accompanying or related message or payment instruction containing only the originator and beneficiary account numbers, provided that:

(a) those details will enable the transaction to be traced back to the originator and beneficiary; and

(b) the originating institution provides the relevant transfer information within 3 business days of a request from the beneficiary institution or the Regulator, and immediately upon request from a law enforcement agency.

(5) Where an Authorised Person or Recognised Body becomes aware that the beneficiary institution is unable to receive relevant transfer information, it must:

(a) use best efforts to communicate the relevant transfer information to the beneficiary institution by other means; and

(b) consider ceasing to make VA/FRT transfers to that beneficiary institution.

(6) An Authorised Person or Recognised Body must not effect a VA/FRT transfer where it is unable to comply with the requirements of Rule 10.3.4.

Guidance

1. For the purposes of collecting, verifying and transmitting relevant transfer information with a VA/FRT transfer, the originator's residential or business address should be the address that the Authorised Person or Recognised Body has verified as part of its CDD on the originator.

2. Due diligence for the purposes of Rule 10.3.4(1)(b) should include, at a minimum:

(a) collecting sufficient information about the beneficiary institution to understand:

(i) the nature of its business;
(ii) its reputation and regulated status; and
(iii) the adequacy and effectiveness of the AML/TFS regulation and supervision applying to it in the jurisdiction(s) in which it operates including whether it is subject to legislation that is equivalent to the standards set out in the FATF Recommendations;

(b) determining the nature and expected volume and value of the VA/FRT transfer(s) involving that beneficiary; and

(c) assessing the beneficiary institution's money laundering controls to ensure they are adequate and effective.

10.3.5 **Additional requirements for the beneficiary institution**

(1) An Authorised Person or Recognised Body must identify and, subject to (2), verify the identity of the beneficiary if the identity has not previously been verified.

(2) An Authorised Person or Recognised Body is not required to verify the identity of the beneficiary where the daily aggregated value of VA/FRT transfers for that beneficiary is less than USD 1,000, and none of the transfers are suspicious transactions.

(3) An Authorised Person or Recognised Body must take reasonable measures, including post-event monitoring or real-time monitoring, where feasible, to identify VA/FRT transfers that lack relevant transfer information.

(4) Where an Authorised Person or Recognised Body becomes aware that relevant transfer information is missing from a VA/FRT transfer, it must:

(a) request that the originating institution provide the relevant transfer information;

(b) quarantine the VA/FRT transfer and delay making the proceeds available to the customer until the relevant transfer information is received; and

(c) consider whether to reject or return the VA/FRT transfer (if technically possible) where the relevant transfer information is not provided within a reasonable time.

(5) An Authorised Person or Recognised Body must report to the Regulator:

(a) any systemic failure by an originating institution to provide required transfer information in connection with VA/FRT transfers; and

(b) the steps taken by the Authorised Person or Recognised Body in response to such failure.

10.3.6 **Requirements for unhosted wallets**

(1) An Authorised Person or Recognised Body must conduct Enhanced CDD on its customer before sending or receiving a VA/FRT transfer to or from an unhosted wallet on behalf of that customer.

(2) Where an Authorised Person or Recognised Body is instructed to effect a VA/FRT transfer to an unhosted wallet, it must:

(a) request any of the relevant transfer information that it does not already hold; and

(b) not proceed with the VA/FRT transfer until such information is provided.

(3) Where an Authorised Person or Recognised Body receives a VA/FRT transfer from an unhosted wallet without relevant transfer information or before undertaking Enhanced CDD on the relevant customer, it must:

(a) take reasonable steps to obtain the missing relevant transfer information from the customer;

(b) quarantine the VA/FRT transfer and delay making the proceeds available to the customer until the relevant transfer information is received or Enhanced CDD has been completed, as applicable; and

(c) consider whether to reject or return the transfer (if technically possible) where the relevant transfer information is not provided or Enhanced CDD

is not completed within a reasonable time, or where the outcome of Enhanced CDD is not satisfactory.

Guidance

When considering whether to reject, return or cease undertaking VA/FRT transfers under Rules 10.3.4(5)(b), 10.3.5(4) and 10.3.6(3), an Authorised Person or Recognised Body should have regard to relevant factors including:

(a) relevant risk assessments it has conducted or should conduct, such as:

(i) an assessment of the level of money laundering risk arising from the relevant VA/FRT transfer;

(ii) the results of relevant customer risk assessments and CDD;

(b) the frequency of VA/FRT transfers involving the customer;

(c) the value of the relevant VA/FRT transfer and any linked or potentially linked transfers; and

(d) relevant communication with the counterparty institution when risk assessing that counterparty.

...

11.1.1 (1) A Relevant Person must 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 which it is required to comply with, under legislation applicable in ADGM or any other jurisdiction.

(2) The systems and controls referred to in (1) must enable the Relevant Person to comply with the requirements in Article 21 of Cabinet Resolution No. (74) of 2020.

(~~2~~3) A Relevant Person must immediately notify the Regulator when it becomes aware that it is, for or on behalf of a Person:

(a) carrying on or about to carry on an activity;

(b) holding or about to hold money or other assets; or

(c) undertaking or about to undertake any other business whether or not arising from or in connection with (a) or (b);

where such carrying on, holding or undertaking constitutes or may constitute a contravention of any Sanctions with which the Relevant Person is required to comply, under legislation applicable in ADGM or any other jurisdiction.

(~~3~~4) A Relevant Person must ensure that the notification stipulated in (2) above includes the following information:

(a) a description of the relevant activity in (2)(a), (b) or (c); and

(b) the action proposed to be taken or that has been taken by the Relevant Person with regard to the matters specified in the notification.

Guidance

1. In Rule 11.1.1(1), taking reasonable measures to comply with resolutions or Sanctions may include, for example, a Relevant Person not undertaking a transaction for or on behalf of a Person without undertaking further due diligence in respect of that Person.

...

5. The ~~systems and controls referred to in Rule 11.1.1(1) should enable a Relevant Person to comply with the~~ requirements of Article 21 of Cabinet ~~Decision~~Resolution No. (74) of 2020~~, which~~ include:

   (a) Registering on the EOCN website to receive updates on changes to Targeted Financial Sanctions lists.

   (b) Regularly screening its databases and transactions against Targeted Financial Sanctions lists as required by the screening scope and timings as set out in the Cabinet ~~Decision~~Resolution.

   (c) Implementing freezing measures without delay or prior notice to the relevant Person(s) if a match is found as a result of the required screening.

   (d) Lifting freezing measures without delay, where necessary.

   (e) Notifying appropriate regulatory authorities of any of the scenarios set out in the Cabinet ~~Decision~~Resolution including confirmed or partial matches against Targeted Financial Sanctions lists.

   (f) Establishing and implementing internal controls and procedures to ensure compliance with the Cabinet ~~Decision~~Resolution.

   (g) Co-operating with the EOCN and relevant regulatory authorities.

6. Relevant Persons should ensure they are fully aware of and in compliance with the requirements issued pursuant to Federal AML Legislation by the EOCN and other relevant authorities including the requirement to file PNMRs and ~~FFRs~~CNMRs as appropriate. Failure to do so, including failure to file a report relating to a confirmed or partial match with a Targeted Financial Sanctions list, may result in the Regulator taking appropriate action.

11.2 Government, regulatory and international findings

11.2.1 (1) A Relevant Person must 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;

(c) the FIU;

(d) the EOCN;

(e) the NAMLCFTC;

(f) UAE enforcement agencies;

(g) the UNSC;

(h) the FATF;

~~i. (i) the Basel Committee on Banking Supervision;~~

(ji) the Regulator; and

(~~k~~j) any other jurisdiction which promulgates Sanctions to which it is subject,

concerning the matters in (2).

...

~~(4) The systems and controls referred to in (1) must enable the Relevant Person to comply with the requirements of Article 21 of Cabinet Decision No. (74) of 2020.~~

(~~5~~4) A Relevant Person must immediately notify the Regulator in writing if it becomes aware of non-compliance by a Person with a finding, recommendation, guidance, directive, resolution, Sanction, notice or other conclusion and provide the Regulator with sufficient details of the Person concerned and the nature of the non-compliance.

Guidance

1. The purpose of this Rule is to ensure that a Relevant Person takes into consideration the broad range of tools used by competent authorities and international organisations to communicate AML/TFS risks to stakeholders.

2. The Regulator may require enhanced CDD or other specific countermeasures to address risks identified in a specific country or jurisdiction. The Regulator may impose such countermeasures either when called upon to do so by FATF or independently of any FATF request.

3. Relevant Persons considering Transactions or business relationships with Persons located in ~~countries or jurisdictions that have been identified as deficient~~Jurisdictions Under Increased Monitoring or Jurisdictions Subject to a Call for Action, or against which the UAE or the Regulator have outstanding advisories,

should be aware of the background against which the assessments or the specific recommendations have been made. These circumstances should be taken into account in respect of business introduced from such jurisdictions~~, and when receiving inward payments for existing customers or in respect of inter-bank transactions~~. The NAMLCFTC website provides information concerning national AML/TFS initiatives, including countermeasures for high-risk countries and updates on developments for high-risk countries.

~~4. The Relevant Person's MLRO is not obliged to report all Transactions from these countries or jurisdictions to the FIU if they do not qualify as suspicious under Federal AML Legislation (see Chapter 14 on Suspicious Activity/Transaction Reports) unless otherwise instructed to do so by the NAMLCFTC.~~

~~5~~4. Transactions with counterparties located in countries or jurisdictions ~~which~~that were previously, but are no longer, identified as deficient or have been relieved from special scrutiny ~~(for example, taken off sources mentioned in this Guidance)~~ may nevertheless require attention which is higher than normal.

~~6~~5. In order to assist Relevant Persons, the Regulator may publish findings, guidance, directives or Sanctions from UAE authorities, the FATF or other relevant bodies. However, the Regulator expects a Relevant Person to take its own steps in acquiring relevant information from various available sources. For example, a Relevant Person may obtain relevant information from consolidated lists of financial Sanctions published by the European Union, HM Treasury, and OFAC.

~~7~~6. In addition, the systems and controls mentioned in Rule 11.2.1 should be established and maintained by a Relevant Person, taking into account its risk assessment under Chapters 6 and 7. In relation to the term "make appropriate use" in Rule 11.2.1, this may mean that a Relevant Person cannot undertake a Transaction for or on behalf of a Person or that it may need to undertake further due diligence in respect of such a Person.

~~8~~7. A Relevant Person should be proactive in obtaining and appropriately using available national and international information, for example, suspect lists or databases from credible public or private sources with regard to money laundering, including obtaining relevant information from sources mentioned in Guidance 6 above. The Regulator encourages Relevant Persons to perform checks against their customer databases and records for any names appearing on such lists and databases as well as to monitor Transactions accordingly.

~~9~~8. The risk of terrorists entering the financial system can be reduced if Relevant Persons apply effective AML/TFS strategies, particularly with respect to CDD. Relevant Persons should assess which countries carry the highest risks and should conduct an analysis of Transactions from countries or jurisdictions known to be a source of terrorist financing.

~~10~~9. The Regulator may require Relevant Persons to take any special measures it may prescribe with respect to certain types of Transactions or accounts where the Regulator reasonably believes that any of the above may pose a money laundering risks to ADGM.

~~11~~10. Relevant Persons are required to have arrangements in place to ensure the ability to comply with all applicable Sanctions in relation to physical delivery of commodities, including Spot Commodities.

~~12~~11. Relevant Persons are reminded that the UAE has regulations in place relating to controls on the export and import of dual-use goods. Relevant Persons should ensure they are in compliance with such regulations. The EOCN makes a list of dual-use goods that are subject to export and import controls available on its website.

...

12.1.1 (1) A Relevant Person must appoint an individual as the MLRO who has an appropriate level of seniority, experience and independence to act in the role, with responsibility for implementation and oversight of its compliance with the Rules in the AML Rulebook. It must do so by completing and filing with the Regulator the appropriate form specified by the Regulator for the Regulator's approval.

(2) The MLRO in (1) and Rule ~~12.1.7~~12.1.6 must be resident in the UAE.

12.1.2 The individual appointed as the MLRO of a DNFBP that comprises of one officer, partner, or principal can, with the prior approval of the Regulator, be the same person as the officer, partner or principal of the DNFBP.

~~**12.1.3** The individual appointed as the MLRO of a Representative Office must be the same individual who holds the position of Principal Representative of that Representative Office.~~

Guidance

In appropriate circumstances, the Regulator may, for a limited period, waive the requirement for an MLRO to be resident in the UAE.

~~1. Authorised Persons are reminded that under GEN Rule 5.5.1 the MLRO function is a mandatory appointment. For the avoidance of doubt, the individual appointed as the MLRO of an Authorised Person, other than a Representative Office, is the same individual who holds the Controlled Function of MLRO of that Authorised Person. Authorised Persons are also reminded that the guidance under GEN Rule 5.5.2 sets out the grounds under which the Regulator will determine whether to grant a waiver from the residence requirements for an MLRO. The same guidance is relevant to other Relevant Persons seeking a waiver from the MLRO residence requirements.~~

~~2. The individual appointed as the MLRO of a Recognised Investment Exchange or Recognised Clearing House is the same individual who holds the position of MLRO of that Recognised Investment Exchange or Recognised Clearing House under the relevant MIR Rule.~~

~~12.1.4~~12.1.3 If the MLRO leaves the employment of the Relevant Person, the Relevant Person must immediately appoint a new MLRO or arrange temporary cover for the MLRO appointment.

~~12.1.5~~12.1.4 A Relevant Person, other than a Representative Office, must appoint an individual to act as a deputy MLRO of the Relevant Person to fulfil the role of the MLRO in ~~his~~their absence.

~~12.1.6~~12.1.5 A Relevant Person's MLRO and deputy MLRO must deal with the Regulator in an open and co-operative manner and must disclose appropriately any information of which the Regulator would reasonably be expected to be notified.

Guidance

1. The individual appointed as the deputy MLRO need not apply for the Regulator's approval.

2. A Relevant Person should make adequate arrangements to ensure that it remains in compliance with the AML Rulebook in the event that its MLRO is absent. Adequate arrangements would include appointing a temporary MLRO for the period of the MLRO's absence, or making sure that the Relevant Person's AML/TFS systems and controls allow it to continue to comply with these Rules when the MLRO is absent.

~~12.1.7~~12.1.6 A Relevant Person may outsource the role of MLRO to an individual outside the Relevant Person, provided that the individual under the outsourcing agreement is and remains suitable to perform the MLRO role.

Guidance

Where a Relevant Person outsources specific AML/TFS tasks of its MLRO to another individual or a third-party provider, including the case where they are within its corporate Group, the Relevant Person remains responsible for ensuring that the duties undertaken by the MLRO ensure its compliance with the requirements in the AML Rulebook. The Relevant Person should satisfy itself of the suitability of anyone who acts for it in the role of MLRO.

12.2 Qualities of an MLRO

12.2.1 A Relevant Person must ensure that its MLRO has:

(a) direct access to the Governing Body and ~~its~~ Senior Management;

(b) sufficient and up-to-date qualifications and experience to fulfil the role and appropriate opportunities to undertake training;

(c) sufficient resources, including, if necessary, an appropriate number of appropriately trained Employees to assist in the performance of ~~his~~their duties in an effective, objective and independent manner;

(d) a level of seniority and independence within the Relevant Person to enable him to act on ~~his~~their own authority;

(e) timely and unrestricted access to information the Relevant Person has about the financial and business circumstances of a customer or any Person on whose behalf the customer is or has been acting, sufficient to enable him to carry out ~~his~~their responsibilities in accordance with Rule 12.3.1; and

(f) unrestricted access to relevant information about the features of the Transaction which the Relevant Person has entered into or may have contemplated entering into with or for the customer or a Person on whose behalf a customer is or has been acting.

Guidance

The Regulator considers that a Relevant Person will need to consider this Rule most especially when appointing an outsourced MLRO. Any external MLRO that is appointed will need to have the actual or effective level of seniority that the role requires.

12.3 Responsibilities of an MLRO

12.3.1 A Relevant Person must ensure that its MLRO implements and has oversight of, and is responsible for, the following matters:

(a) the day-to-day operations for compliance by the Relevant Person with its AML/TFS policies, procedures, systems and controls;

(b) acting as the point of contact to receive internal notifications of suspicious activity from the Relevant Person's Employees under Rule 14.2.2;

(c) taking appropriate action under Rule 14.3.1 following receipt of a notification from an Employee;

(d) making, in accordance with Federal AML Legislation, Suspicious Activity/Transaction Reports;

(e) acting as the point of contact within the Relevant Person for competent UAE authorities and the Regulator regarding money laundering issues;

(f) responding promptly to any request for information made by competent UAE authorities or the Regulator;

(g) receiving and acting upon any relevant findings, recommendations, guidance, directives, resolutions, Sanctions, notices or other conclusions described in Chapter 11; ~~and~~

(h) establishing and maintaining an appropriate money laundering training programme and adequate awareness arrangements under Chapter 13~~.~~; and

(i) reviewing and assessing the Relevant Person's AML/TFS policies, procedures, systems and controls for consistency with the AML Rulebook and Federal AML Legislation and, if necessary, recommending updates and enhancements.

~~**Guidance**~~

~~Depending on the size, nature and complexity of the business and operations, Relevant Persons and MLROs should consider whether it is appropriate to screen prospective employees for money laundering risks prior to employment to ensure high standards when hiring.~~

...

12.4.2 A Relevant Person must ensure that its Governing Body or Senior Management promptly:

(a) assess the report provided under Rule 12.4.1;

(b) take action, as required, subsequent to consideration of the findings of the report, in order to resolve any identified deficiencies; and

(c) make a record of their assessment pursuant to ~~paragraph~~ (a) and the action taken pursuant to ~~paragraph~~ (b).

...

13.1.1 A Relevant Person must:

(a) provide AML/TFS training to all relevant Employees at appropriate and regular intervals;

(b) ensure that its AML/TFS training enables its Employees to:

(i) know the identity, and understand the responsibilities, of the Relevant Person's MLRO and ~~his~~their deputy;

...

14.1 Application and definitions

In this Chapter, "money laundering" and "terrorist financing" ~~means~~mean the criminal offences defined in Federal AML Legislation.

...

14.2.2 A Relevant Person must have policies, procedures, systems and controls to ensure that whenever any Employee, acting in the ordinary course of ~~his~~their employment, either:

(a) knows;

(b) suspects; or

(c) has reasonable grounds for knowing or suspecting,

that a Person is engaged in or attempting money laundering or terrorist financing, that Employee promptly notifies the Relevant Person's MLRO and provides the MLRO with all relevant details.

14.2.3 A Relevant Person must have policies and procedures to ensure that disciplinary action can be taken against any Employee who fails to make such a report.

Guidance

1. Circumstances that might give rise to suspicion or reasonable grounds for suspicion of money laundering or terrorist financing include:

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

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

   (c) where the size or pattern of Transactions, without reasonable explanation, is out of line with any pattern that has previously emerged or may have been deliberately structured to avoid detection;

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

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

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

   (g) unnecessary routing of funds through third-party accounts; or

   (h) unusual Transactions without an apparently profitable motive.

...

3. Where appropriate, a Relevant Person should also utilise the methods described in ~~paragraph 1 above~~. to detect a range of Financial Crimes, including fraud. Bearing in mind the evolving nature of Financial Crime and the methods used to further it, a Relevant Person should apply best practice when determining which behaviours would be considered suspicious and what measures are required to detect suspicious activity and Transactions. Such practices may include, but are not limited to, incorporating the analysis of customer behaviour metrics into the monitoring of suspicious activity and Transactions.

...

5. A Relevant Person may allow its Employees to consult with their line managers before sending a report to the MLRO. The Regulator would expect that such consultation does not prevent making a report whenever an Employee has stated that ~~he has~~they have knowledge, suspicion or reasonable grounds for knowing or suspecting that a Person may be involved in money laundering. Whether or not an Employee consults with ~~his~~their line manager or other Employees, the responsibility remains with the Employee to decide for ~~himself~~themselves whether a notification to the MLRO should be made.

...

10. Relevant Persons should comply with guidance issued by the NAMLCFTC, FIU and EOCN ~~with regard to~~about identifying and reporting suspicious activity and Transactions relating to money laundering, terrorist financing and proliferation financing.

...

14.3.4 A Relevant Person must ensure that if the MLRO decides to make a SAR/STR, ~~his~~their decision is made independently and is not subject to the consent or approval of any other Person.

14.3.5 Relevant Persons are required to register on goAML upon receipt of their Financial Services Permission, Recognition Order or registration licence in order to submit SAR/STRs.

Guidance

1. Relevant Persons are reminded that the failure to report suspicions of money laundering or terrorist financing may constitute a criminal offence that is punishable under the laws of the UAE.

~~2. Relevant Persons should comply with guidance issued by the EOCN regarding reporting suspicious activity and Transactions relating to money laundering, terrorist financing and proliferation financing.~~

~~3~~2. SARs/STRs under Federal AML Legislation should be submitted to the FIU via goAML. The dedicated mechanism for registering and reporting on goAML is available on the Regulator's website. Failure to register on goAML may lead to the Regulator taking action.

~~4~~3. In the preparation of a SAR/STR, if a Relevant Person knows or assumes that the funds which form the subject of the report do not belong to a customer but to a third party, this fact and the details of the Relevant Person's proposed course of further action in relation to the case should be included in the report.

~~5~~4. If a Relevant Person has filed a SAR/STR, the FIU may instruct the Relevant Person on how to continue its business relationship, including effecting any Transaction

with a Person. If the customer in question expresses his wish to move the funds before the Relevant Person receives instruction from the FIU on how to proceed, the Relevant Person should immediately contact the FIU for further instructions.

5. Relevant Persons should comply with their internal reporting mechanisms on monitoring transactions and activities pertaining to Jurisdictions Subject to a Call for Action as set out in Rule 4.9.

...

15. DNFBP REGISTRATION AND SUPERVISION

~~**Guidance**~~

~~1. FSMR gives the Regulator the power to supervise DNFBPs' compliance with relevant Federal AML Legislation. FSMR also gives the Regulator a number of other powers in relation to DNFBPs, including powers of enforcement. This includes the power to obtain information and to conduct investigations into possible breaches of FSMR. The Regulator may also impose fines for breaches of FSMR or the Rules. It may also suspend or withdraw the registration of a DNFBP in various circumstances.~~

~~2. The Regulator takes a risk-based approach to regulation of persons which it supervises. Generally, the Regulator will work with DNFBPs to identify, assess, mitigate and control relevant risks where appropriate. The Guidance & Policies Manual ("**GPM**") describes the Regulator's enforcement powers under FSMR and outlines its policy for using these powers.~~

~~3. Rule 15.1.1 requires a DNFBP to be registered by the Regulator to conduct its activities in ADGM. Rule 15.2.1 sets out the criteria a DNFBP must meet to be registered. The Regulator may suspend or withdraw the registration of a DNFBP where the DNFBP no longer meets the criteria for registration.~~

~~4. A DNFBP is defined in Rule 3.2.1 and includes the following class of persons whose business is carried out in ADGM:~~

~~i. (a) a real estate agency which carries out transactions with other Persons that involve the acquiring or disposing of real property;~~

~~ii. (b) a dealer in precious metals or precious stones;~~

~~iii. (c) a dealer in any saleable item of a price equal to or greater than USD15,000;~~

~~iv. (d) an accounting firm, audit firm, insolvency firm or taxation consulting firm;~~

~~v. (e) a law firm, notary firm or other independent legal business; or~~

~~vi. (f) a Company Service Provider.~~

~~5. In determining if a Person is a DNFPB the Regulator will adopt a 'substance over form' approach. That is, it will consider what business or profession is in fact being carried on, and its main characteristics, and not just what business or profession the Person purports, or is licensed, to carry on in ADGM.~~

~~6. The Regulator considers that a "law firm, notary firm or other independent legal business, includes any business or profession that involves a legal service, including advice or services related to laws in the UAE The Regulator does not consider it necessary for the purposes of the definition that the:~~

~~(a) Person is licensed to provide legal services in the UAE; or~~

~~(b) the individuals or employees providing the legal service are qualified or authorised to do so.~~

~~7. The Regulator considers that "accounting firm, audit firm, insolvency firm or taxation consulting firm", includes forensic accounting services that use accounting skills, principles and techniques to investigate suspected illegal activity or to analyse financial information for use in legal proceedings.~~

~~15.1 DNFBP prohibition~~

~~**15.1.1** A Person who is a DNFBP must not carry on any activities in or from ADGM unless that Person is registered under AML 15.4 by the Regulator as a DNFBP.~~

~~**15.1.2** The Regulator may delegate its powers for the registration, suspension and cancellation of a DNFBP's registration to the Registrar of Companies.~~

~~**15.2**~~

15.1 Criteria for registration as a DNFBP

~~**15.2.1**~~

15.1.1 (1) To be registered as a DNFBP, an applicant must demonstrate to the Regulator's satisfaction that:

(a) it is fit and proper to perform AML/TFS functions; and

(b) it has adequate resources, systems and controls, including policies and procedures, to comply with all applicable AML/TFS requirements under Federal AML Legislation, FSMR and these Rules;

(2) In assessing ~~if~~whether an applicant is fit and proper under (1)(a), the Regulator may, without limiting the matters it may take into account ~~under that paragraph~~, consider the applicant, its ~~senior management,~~Governing Body, its Senior Management, its Beneficial Owners, other entities in its Group and any other Person with whom it has a relationship.

(3) The Regulator will, in assessing ~~if an applicant is fit and proper~~the matters in (1), consider the cumulative effect of ~~matters that, if considered~~factors which, if taken individually, may be regarded as insufficient to give reasonable cause to doubt the fitness and propriety of ~~the~~an applicant.

~~15.3~~15.2 Application for registration as a DNFBP

~~**15.3.1** A Person may apply to the Regulator to be registered as a DNFBP by completing and submitting the appropriate form.~~

15.2.1 A Person seeking registration as a DNFBP must complete and submit to the Regulator an application in such form as the Regulator shall prescribe.

~~**15.3.2**~~15.2.2 The Regulator may require an applicant to provide additional information or documents reasonably required by the Regulator for it to be able to consider an application for registration including, but not limited to, information or documents relating to the activities, ownership, group structure, financial and other resources of the applicant.

~~**15.3.3**~~15.2.3 Where, at any time between filing an application and the grant or refusal of registration as a DNFBP, an applicant becomes aware of a material change in its circumstances that is reasonably likely to be relevant to its application it shall inform the Regulator in writing of the change without delay.

~~**15.3.4** Any Person who is a DNFBP upon the making of this Chapter and was previously a Relevant Person prior to the making of this Chapter:~~

~~(a) is deemed to be registered as a DNFBP at the time of the making of this Chapter; and~~

~~(b) must apply for registration under Rule 15.3:~~

~~(i) within 12 months of the making of this Chapter; or~~

~~(ii) at the date of the renewal of its Commercial Licence under the Commercial Licensing Regulations;~~

~~whichever comes first.~~

~~15.4 Grant of an application~~

~~**15.4.1** The Regulator may grant an application for DNFBP registration as a DNFBP if it is satisfied that the applicant meets the criteria for registration under Rule 15.2.~~

~~**15.4.2** Where the Regulator decides to register a DNFBP, it shall as soon as is practicable inform the applicant in writing of that decision and of the date on which registration is to take effect.~~

~~**15.5 Refusal of an application**~~

~~**15.5.1** The Regulator may refuse to grant an application for DNFBP registration where it is not satisfied that the applicant meets the criteria for registration under Rule 15.2.~~

~~15.6~~15.3 DNFBP notifications

~~**15.6.1**~~15.3.1 A DNFBP must promptly notify the Regulator of any change in its:

(a) name;

(b) legal status;

(c) address;

(d) MLRO;

(e) ~~senior management~~Governing Body; ~~or~~

(f) Senior Management; or

(~~f~~g) Beneficial ~~ownership~~Ownership.

~~**15.6.2**~~15.3.2 (1) A DNFBP must notify the Regulator in writing at least ten Business Days in advance of it ceasing to carry on the business activities that establish it as a DNFBP.

(2) The notice must include a request to cancel its registration, an explanation of the reason for the DNFBP ceasing business, the planned date of the cessation of its activities, and copies of any relevant documents must be submitted with the notice.

~~**15.7 Suspension and withdrawal of DNFBP registration**~~

~~**15.7.1** (1) The Regulator may suspend the registration of a DNFBP at the request of the DNFBP or on its own initiative.~~

~~8. (2) The Regulator may withdraw the registration of a DNFBP:~~

~~(a) at the request of the DNFBP;~~

~~(b) if the Registrar of Companies notifies it that the DNFBP no longer holds the relevant commercial licence to operate in ADGM; or~~

~~(c) on its own initiative.~~

~~**15.7.2** (1) The Regulator may exercise its power on its own initiative under Rule 15.7.1 (1) or (2)(c) where:~~

~~(a) the DNFBP no longer meets the criteria for DNFBP registration;~~

~~(b) the DNFBP is in breach of, or has been in breach of, ADGM legislation including any Rules or any other legislation applicable in ADGM including Federal AML Legislation;~~

~~(c) the DNFBP is insolvent or entering into administration;~~

~~(d) the DNFBP is no longer carrying on business in ADGM; or~~

~~(e) the Regulator considers that exercising the power is necessary or desirable in the pursuit of its objectives in section 1(3) of FSMR.~~

~~**Guidance**~~

~~1. A DNFBP may request the withdrawal of its registration because, for example, it no longer meets the definition of a DNFBP, becomes insolvent or enters into administration, or proposes to leave ADGM.~~

~~2. In addition to being able to withdraw registration at the request of a DNFBP, the Regulator may, on its own initiative, suspend or withdraw the registration of a DNFBP in various circumstances.~~

~~15.8~~15.4 Disclosure of regulatory status

~~15.8.1~~15.4.1 A DNFBP must not:

(a) misrepresent its regulatory status with respect to the Regulator expressly or by implication; or

(b) use or reproduce the logo of the Regulator without express written permission from the Regulator and in accordance with any conditions for use imposed by the Regulator.

~~15.9~~15.5 Co-ordination between the Regulator and the Registrar of Companies

~~15.9.1~~15.5.1 (1) The Registrar of Companies shall not grant a Person who is a DNFBP a commercial licence to operate in ADGM until the Regulator has confirmed to the Registrar of Companies that it intends to register the Person as a DNFBP.

(2) The Regulator shall as soon as is practicable notify the Registrar of Companies where it suspends or withdraws the registration of a DNFBP.

(3) The Registrar of Companies shall as soon as is practicable suspend or withdraw (as the case may be) the commercial licence of the DNFBP where it receives a notification under (2).

Guidance

1. FSMR prohibits a DNFBP from conducting its business in ADGM unless it is registered by the Regulator. Section 7(6) of FSMR gives the Regulator the power to make Rules in connection with the creation and implementation of anti-money laundering measures, including criteria for the registration of DNFBPs.

2. Section 15A of FSMR designates the Regulator as the supervisory authority for licensing and supervising DNFBPs in ADGM for the purposes of Federal AML Legislation, other than Legal Professionals. The Ministry of Justice may delegate some of its powers as supervisory authority for Legal Professionals to the Regulator or the Registrar of Companies from time to time.

3. Section 15B of FSMR sets out the overarching anti-money laundering obligations of Relevant Persons in ADGM, including DNFBPs. Sections 15C and 15D of FSMR govern registration as a DNFBP in ADGM. DNFBPs should refer to FSMR to ensure an understanding of these provisions.

4. Pursuant to section 15E of FSMR, the Regulator has delegated its powers to supervise and register DNFBPs pursuant to Anti-Money Laundering Legislation to the Registrar of Companies. Accordingly, applications for registration as a DNFBP should be made to the Registrar of Companies.

5. FSMR gives the Regulator other powers in relation to DNFBPs, including powers of enforcement. This includes the power to obtain information and conduct investigations into possible breaches of FSMR, including breaches of the AML Rulebook. The Regulator has not delegated its enforcement powers to the Registrar of Companies.

6. The Guidance & Policies Manual (GPM) describes the Regulator's enforcement powers and outlines its policy for using these powers. Where the Regulator, or the Registrar of Companies on its behalf, refuses to grant an application for DNFBP registration, the procedures set out in Part 21 of FSMR will apply.

7. In determining whether a Person is a DNFBP, the Regulator will adopt a 'substance over form' approach. That is, it will consider what business or profession is in fact being carried on, and its main characteristics, and not just what business or profession the Person purports, or is licensed, to carry on in ADGM.

8. The Regulator considers that a Legal Professional includes any business or profession that involves a legal service, including advice or services related to laws in the UAE. The Regulator does not consider it necessary for the definition of a Legal Professional that the:

   (a) Person is licensed to provide legal services in the UAE; or

   (b) the individuals or employees providing the legal service are qualified or authorised to do so.

9. The Regulator considers that an "accounting firm, audit firm, insolvency firm or taxation consulting firm", includes firms providing forensic accounting services

that use accounting skills, principles and techniques to investigate suspected illegal activity or to analyse financial information for use in legal proceedings.

10. A DNFBP may request the withdrawal of its registration because, for example, it no longer meets the definition of a DNFBP, becomes insolvent or enters into administration, or proposes to leave ADGM.

11. In addition to being able to withdraw registration at the request of a DNFBP, the Regulator may, on its own initiative, suspend or withdraw the registration of a DNFBP in various circumstances. Where it does so on its own initiative, the procedures set out in Part 21of FSMR will apply.

12. DNFBPs may be subject to additional conduct of business requirements pursuant to ADGM commercial legislation, including restrictions on dealing in cash in relation to certain Transactions. DNFBPs should make themselves aware of and comply with such requirements, which the Registrar supervises.

...

16.1.2 An NPO must maintain information on the following:

(a) the purpose and objectives of its stated activities;

(b) the identity of the persons who own, control or direct its activities, including the Governing Body and ~~senior management~~Senior Management;

(c) the relevant controls that have been put in place to ensure that all funds are fully accounted for, and are spent in a manner that is consistent with the purpose and objectives of its stated activities; and

(d) the relevant measures that it has taken to confirm the identity, credentials and good standing of beneficiaries and associated NPOs to ensure that they are not involved with terrorists or terrorist organisations and that its charitable funds are not used to support terrorists or terrorist organisations.

...

16.3.2 An NPO must, at the request of the Regulator:

(a) give or procure the giving of specified information, Documents, files, tapes, computer data or other material in the NPO's possession or control to the Regulator;

...

Guidance

1. An NPO should have systems and controls in place to identify donors, including where a donor is resident and, where the donor is not a Natural Person, the activities it undertakes.

2. An NPO should take into consideration money laundering risks posed by a donor, including as a result of the jurisdiction in which the donor is resident or the activities the donor undertakes.

3. Where a donor is resident in a high-risk jurisdiction, an NPO should conduct a risk-based assessment to identify money laundering risks posed by that donor.

4. An NPO should encourage donors to make donations through financial channels offered by Financial Institutions regulated by the Regulator or ~~another~~a Non-ADGM Financial Services Regulator.

5. An NPO should implement other focused, proportionate and risk-based measures as appropriate.

6. Pursuant to section 15E of FSMR, the Regulator has delegated its powers to register and supervise NPOs in relation to AML/TFS to the Registrar of Companies.

...