# Anti-Money Laundering and Sanctions Rulebook (AML)

**(VER11.210526)**

## TABLE OF CONTENTS

The contents of the AML Rulebook are divided into the following Chapters and sections:

# 1. INTRODUCTION

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

## 1.1 Jurisdiction

1.1.1 (1) The AML Rulebook is made in recognition of the application of the Federal AML Legislation in ADGM.

(2) Nothing in the AML Rulebook affects the operation of Federal AML Legislation.

## 1.2 Application

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

(a) every Relevant Person in respect of all its activities carried out in or from ADGM; and

(b) the Persons specified in Rule 1.3.3 as being responsible for a Relevant Person's compliance with the AML Rulebook.

(2) In respect of a Relevant Person that is:

(a) an Authorised Person, other than a Credit Rating Agency, and a Recognised Body, only the requirements of Chapters 1 to 14 of the AML Rulebook apply;

(b) a Representative Office, only the requirements of Chapters 1 to 6 and 11 to 14 of the AML Rulebook apply;

(c) a DNFBP, only the requirements of Chapters 1 to 9 and 11 to 15 of the AML Rulebook apply; and

(d) an NPO, only the requirements of Chapter 16 of the AML Rulebook apply.

**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 transfers of Virtual Assets and Fiat-Referenced Tokens, as well as audit, and anonymous and nominee accounts.

3. Relevant Persons should consider these Chapters and determine which provisions apply. To assist Relevant Persons the following table sets out the application of the

AML Rulebook to each of the different types of Relevant Persons specified in Rule 1.2.1(1). This table is for guidance purposes only.

**Application table**

| Relevant Person | Applicable Chapter(s) | |
|---|---|---|
| Authorised Person, other than a Credit Rating Agency, or Recognised Body | 1 - 14 | |
| Representative Office | 1 - 6 | 11 - 14 |
| DNFBP | 1 - 9 | 11 - 15 |
| NPO | 16 | |

## 1.3 Responsibility for compliance with the AML Rulebook

1.3.1 A Relevant Person's Governing Body is responsible for establishing, maintaining and monitoring the Relevant Person's AML/TFS policies, procedures, systems and controls and compliance with the AML Rulebook, FSMR, and all applicable Federal AML Legislation.

1.3.2 A Relevant Person's Governing Body must ensure the policies, procedures, systems and controls referred to in Rule 1.3.1 are effective to meet the obligations of the Relevant Person.

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.

(3) Nothing in this Rule precludes the Regulator from taking enforcement action against any Person, including any one or more of the following Persons, in respect of a breach of any Rule in the AML Rulebook:

(a) a Relevant Person;

(b) members of a Relevant Person's Senior Management; or

(c) an Employee of a Relevant Person.

## 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 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, 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.

4. Particular legislation to be aware of includes:

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

   (b) Cabinet 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); and

   (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).

5. 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 ensure they are aware of, and comply with, all notices issued by the Regulator and applicable decisions, guidance and guidelines issued by governmental authorities in the UAE pursuant to Federal AML Legislation.

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**

12. Chapter 2 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.

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

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

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.

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.

17. Chapter 10 sets out obligations on Authorised Persons and Recognised Bodies in relation to correspondent banking, electronic fund transfers, transfers of Virtual Assets and Fiat-Referenced Tokens, and audit requirements.

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).

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

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).

21. Chapter 14 contains the obligations applying to all Relevant Persons concerning SAR/STRs, which are required to be made under Federal AML Legislation.

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

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.

25. Under Article 4 of the AML Law, 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.

26. Under Article 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**

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. 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 to assist it in complying with these Rules.

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**

30. The Basel Committee on Banking Supervision has published guidelines for banks related to money laundering and terrorist financing, which are intended to supplement the FATF Recommendations. Banks in ADGM should read these Rules in conjunction with those guidelines and the FATF Recommendations.

**Wolfsberg Group**

31. The Wolfsberg Group is an association of global banks that has published guidance aimed at assisting financial institutions in managing money laundering risks and preventing terrorist financing. Banks operating in ADGM should be familiar with the

relevant Wolfsberg Group guidance, published in conjunction with the FATF Recommendations, and with the Rules.

**Sanctions**

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 are Sanctions issued by the UNSC or the UAE involving asset freezing and other financial prohibitions targeted at individuals, entities or groups to combat terrorism and terrorist financing, and countering the proliferation of WMD. 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.

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. and the U.S. 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. INTERPRETATION AND TERMINOLOGY

### 3.1 Interpretation

3.1.1 Further to section 15A(1) of FSMR, a reference in the AML Rulebook to "money laundering" 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 Glossary for AML

**Guidance on the term "customer"**

1. The point at which a Person becomes a customer will vary from business to business. However, the Regulator considers that it would usually occur at or prior to the business relationship being formalised, for example, by the signing of a client agreement or the acceptance by the customer of terms of business.

2. The Regulator does not consider that a Person would be a customer of a Relevant Person merely because such Person receives marketing information from a Relevant Person or where a Relevant Person refers a Person who is not a customer to a third party, including a Group member.

3. The Regulator considers that a Counterparty would generally be a customer for the purposes of the AML Rulebook and would therefore require a Relevant Person to undertake CDD on such a Person. However, this would not include a counterparty in a Transaction undertaken on a Regulated Exchange. Nor would it include suppliers of ancillary business services for consumption by the Relevant Person, such as cleaning, catering, stationery, IT or other similar services.

4. A Representative Office should not have any customers in relation to its ADGM operations.

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

| Term | Definition |
|---|---|
| ADGM | Means the Abu Dhabi Global Market. |
| ADGM Board | Means the Board of Directors of ADGM. |
| ADGM Entity | Means a Legal Person which is incorporated or registered in ADGM, excluding a registered Branch. |

| Term | Definition |
|---|---|
| AML Law | Means Federal Decree by Law No. (10) of 2025 Concerning Combatting Money Laundering, 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. |
| AML Return | Means the return which is required to be completed by Relevant Persons in accordance with Rule 4.6. |
| AML Rulebook | Means this Anti-Money Laundering and Sanctions Rulebook. |
| AML/TFS | Means anti-money laundering, including measures undertaken against terrorist financing, proliferation financing, financing of unlawful organisations and sanctions non-compliance, and the observance of and compliance with applicable Sanctions including Targeted Financial Sanctions. |
| Anti-Money Laundering Legislation | Means:<br>(a) Federal AML Legislation; and<br>(b) legislation administered by the Regulator relating to combatting money laundering, including this AML Rulebook. |
| Authorised Person | Means a Person, other than a Recognised Body, who is authorised under the FSMR. |
| Beneficial Owners | Means, in relation to a customer, a Natural Person who ultimately owns or controls the customer or a Natural Person on whose behalf a transaction is conducted or a business relationship is established and includes:<br>(a) in relation to a body corporate, a Person referred to in Rule 8.3.3(2);<br>(b) in relation to a Partnership, a Person referred to in Rule 8.3.4(2);<br>(c) in relation to a trust or other similar Legal Arrangement, a Person referred to in Rule 8.3.5(2); and |

| Term | Definition |
|---|---|
| | (d) in relation to a foundation, a Person referred to in Rule 8.3.6(2). |
| 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. |
| Client | Means a Retail Client, Professional Client or Market Counterparty as defined in COBS 2. |
| Client Agreement | Means an agreement between an Authorised Person and a Client which is made or entered into in accordance with COBS 3.3. |
| Client Money | Means money of any currency which an Authorised Person holds on behalf of a Client, including any receivables of the Authorised Person in respect of bank accounts or clearing or brokerage accounts, or which an Authorised Person treats as Client Money, subject to the exclusions in COBS 14.2.6. |
| CNMR | Means a confirmed name match report to be filed via goAML in the prescribed format. |
| COBS | Means the Conduct of Business Rulebook. |
| Company | Includes:<br>(a) any Body Corporate wherever incorporated; and<br>(b) any unincorporated body constituted under the law of a country, territory or jurisdiction outside ADGM. |
| Company Service Provider | Means a Person that carries out the following services on behalf of a customer:<br>(a) acting as a formation agent of Legal Persons;<br>(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;<br>(c) providing a registered office, business address or accommodation, correspondence or administrative |

| Term | Definition |
|---|---|
| | address for a company, a partnership or any other Legal Person or Legal Arrangement; or<br><br>(d) acting as, or arranging for another Person to act as, a nominee shareholder for another Person. |
| Contract of Insurance | Has the meaning given in Part 4 of Schedule 1 of FSMR. |
| Contravention | Means a contravention of any Regulations or Rules made by the ADGM Board and the Regulator, as the case may be. |
| Correspondent Account | Means an account opened by a Correspondent Bank to receive deposits from, to make payments on behalf of or to otherwise handle financial transactions for or on behalf of the Respondent as part of the provision of Correspondent Banking services. |
| Correspondent Bank | Means the correspondent Financial Institution in a Correspondent Banking relationship. |
| Correspondent Banking | Means the provision of banking services by a correspondent Financial Institution to a respondent Financial Institution and other similar relationships. |
| Counterparty | Means any Person with or for whom an Authorised Person carries on, or intends to carry on, any regulated business or associated business. In this context, a Counterparty includes an individual, unincorporated association, Company, government, local authority or other public body. |
| Credit Rating Agency | Means a Person carrying on, in or from ADGM, the Regulated Activity of Operating a Credit Rating Agency for which it has an authorisation under its Financial Services Permission. |
| Customer Due Diligence (CDD) | 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 class of Persons who carry out any of the following businesses in ADGM:<br><br>(a) a real estate agency which carries out transactions for or on behalf of a customer involving the buying or selling of real property;<br><br>(b) a dealer in precious metals or precious stones; |

| Term | Definition |
|---|---|
| | (c) a dealer in any saleable item of a price equal to or greater than USD15,000;<br><br>(d) an accounting firm, audit firm, insolvency firm or taxation consulting firm;<br><br>(e) a Legal Professional; or<br><br>(f) a Company Service Provider. |
| Director | Means:<br><br>(a) in relation to an Undertaking established under the ADGM Companies Regulations, a Person who appears on the Register of Directors maintained by the Registrar of Companies;<br><br>(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 or performs the function of acting in the capacity of a Director, by whatever name called;<br><br>(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<br><br>(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. |
| eKYC | Means verification of customer identity by way of electronic, non-face-to-face means only. |
| eKYC System | Means the technology and associated processes used to undertake eKYC. |
| Employee | Means an individual:<br><br>(a) 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<br><br>(b) whose services, under an arrangement between that Person and a third party, are placed at the disposal and under the control of that Person. |

| Term | Definition |
|---|---|
| Enhanced Customer Due Diligence (Enhanced CDD) | Means undertaking Standard CDD and, in addition, the enhanced measures under Rule 8.4. |
| EOCN | Means the Executive Office for Control and Non-Proliferation of the UAE. |
| FATF | Means the Financial Action Task Force. |
| FATF Recommendations | Means the publication entitled the "International Standards on Combatting Money Laundering and the Financing of Terrorism & Proliferation", as published and amended by the FATF. |
| Federal AML Legislation | Means the legislation described in section 258 of FSMR. |
| Fiat-Referenced Token | Has the meaning given in section 258 of FSMR. |
| Financial Crime | Includes any offence involving:<br>(a) fraud or dishonesty;<br>(b) misconduct in or misuse of information relating to a financial market;<br>(c) handling the proceeds of crime; or<br>(d) the financing of terrorism. |
| Financial Institution | Means:<br>(a) (i) an Authorised Person;<br>(ii) a Recognised Body; or<br>(iii) any Person that carries out as its principal business an activity which would be a Regulated Activity or would require a Recognition Order if carried out in ADGM; and<br>(b) that is not one of the following:<br>(i) a governmental organisation, including the Central Bank of the UAE or its equivalent in any state; or<br>(ii) a multilateral development bank. |
| Financial Services Permission | Means a permission given, or having effect as if so given, by the Regulator in accordance with Part 4 of FSMR. |

| Term | Definition |
|---|---|
| FIU | Means the Financial Intelligence Unit of the UAE. |
| FSMR | Means the Financial Services and Markets Regulations 2015. |
| goAML | Means the federally mandated reporting portal administered by the FIU, and any successor portal, platform or reporting tool. |
| Governing Body | Means the board of directors, partners, committee of management or other governing body of an Undertaking. |
| Group | Has the meaning given in section 258 of FSMR. |
| Guidance | Has the meaning given in section 15(2) of FSMR. |
| HM Treasury | Means the UK government's economic and finance ministry. |
| IMF | Means the International Monetary Fund. |
| International Organisation | Means an organisation established by formal political agreement between member countries, where the agreement has the status of an international treaty, and the organisation is recognised in the law of countries which are members. |
| Jurisdiction Subject to a Call for Action | Means a jurisdiction identified by the FATF as a 'high-risk jurisdiction subject to a call for action' or any equivalent list issued by the FATF. |
| Jurisdiction Under Increased Monitoring | Means a jurisdiction identified by the FATF as a 'jurisdiction under increased monitoring' or any equivalent list issued by FATF. |
| Legal Arrangement | Means express trusts or other similar legal arrangements. |
| 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, unincorporated bodies, foundations, partnerships, associations, states and governments and other similar entities. |
| Legal Professional | Means a law firm, notary firm or other independent legal business whose business is carried out in the ADGM. |

| Term | Definition |
|---|---|
| Listed Body Corporate | Means, for the purposes of Rule 8.3.3(4), a Body Corporate listed on a stock exchange recognised by the Regulator. |
| Local Terrorist List | Means the UAE's national terrorist list issued by the UAE Cabinet. |
| MIR | Means the Market Infrastructure Rulebook. |
| MLRO | Means 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 or Recognised Body, includes a Money Laundering Reporting Officer as that term is defined in GLO. |
| NAMLCFTC | Means the National Anti-Money Laundering and Combatting Financing of Terrorism and Financing of Illegal Organizations Committee of the UAE. |
| Natural Person | Means an individual. |
| Non-ADGM Financial Services Regulator | Has the meaning given in section 258 of FSMR. |
| Non-Face-to-Face (NFTF) | Where a customer is not physically present for a business operation or transaction with a Relevant Person. |
| Non-Profit Organisation (NPO) | Means an organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes or for other charitable purpose. |
| OECD | Means the Organisation for Economic Co-operation and Development. |
| OFAC | Means the Office of Foreign Assets Control of the U.S. Department of the Treasury. |
| Parent | Means a Holding Company as defined in section 1015 of the Companies Regulations. |
| Partner | Means, in relation to an Undertaking which is a Partnership, a Person occupying the position of a partner, by whatever name called. |
| Partnership | Means any partnership, including a partnership constituted under the law of a country, jurisdiction or territory outside ADGM, but not including a Limited Liability Partnership. |

| Term | Definition |
|---|---|
| Payment Transaction | Has the meaning given in section 258 of FSMR. |
| Penal Code | Means Federal Law No. (31) of 2021 (the Penal Code of the UAE). |
| Person | Means a person and includes any Natural Person, any Legal Person and any Legal Arrangement. |
| PNMR | Means partial name match report to be filed via goAML in the prescribed format. |
| Politically Exposed Person (PEP) | Means a Natural Person:<br>(a) 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 government, a senior politician, a senior governmental, military, diplomatic or judicial official, a senior executive of a state-owned corporation, an important political party official; or<br>(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 or more junior individuals in categories (a) or (b), and<br>(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. |
| Recognised Body | Means a Recognised Investment Exchange or a Recognised Clearing House. |
| Recognition Order | Has the meaning given in section 258 of FSMR. |
| Registrar of Companies | Means the ADGM Registrar of Companies. |
| Regulated Activity | Has the meaning given in section 19 of FSMR. |
| 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 a Non-ADGM Financial Services Regulator. |

| Term | Definition |
|---|---|
| Regulation | Means any regulation made by the ADGM Board. |
| Regulator | Means the ADGM Financial Services Regulatory Authority. |
| Relevant Person | Has the meaning given in section 258 of FSMR. |
| Representative Office | Means the business operations of Person authorised to carry on the Regulated Activity of Operating a Representative Office in ADGM and which actually carries on the Regulated Activity of Operating a Representative Office. |
| Respondent Bank | Means the respondent Financial Institution in a Correspondent Banking relationship. |
| Restricted Scope Company | Has the meaning given in section 3(4) of the Companies Regulations. |
| Rule | Means any rule made by the Regulator or the ADGM Board, as applicable, in accordance with Part 2 of FSMR. |
| Sanctions | Means any law executing foreign policy, security, sanction, trade embargo, or anti-terrorism objectives or similar restrictions imposed, administered or enforced from time to time by:<br>(a) the UAE;<br>(b) the United Nations Security Council;<br>(c) the European Union;<br>(d) HM Treasury of the United Kingdom;<br>(e) the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury;<br>(f) any other relevant governmental authority;<br>(g) any relevant inter-governmental or supra-national authority; or<br>(h) any of their successors. |
| Sanctions List | Means any official list of Persons, entities or groups targeted by Sanctions. |

| Term | Definition |
|---|---|
| Senior Management | Means:<br><br>(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.<br><br>(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. |
| Shareholder | Has the meaning given in section 258 of FSMR. |
| 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 Standard CDD that has been modified pursuant to the operation of Rule 8.5. |
| 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. |
| Source of Wealth | Means how the customer's global wealth or net worth is or was acquired or accumulated. |
| Spot Commodity | Has the meaning given in section 258 of FSMR. |
| SAR/STR | Means a suspicious activity or transaction report to be made via goAML to the FIU in the prescribed format. |
| Standard Customer Due Diligence (Standard CDD) | Means CDD carried out pursuant to Rule 8.3. |
| Targeted Financial Sanctions | Means financial Sanctions issued by the UNSC or the UAE against specific individuals, entities or groups to combat terrorism, terrorist financing and the proliferation of WMD, |

| Term | Definition |
|---|---|
| | 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. |
| Transaction | Means any transaction undertaken by a Relevant Person for or on behalf of a customer in the course of carrying on a business in or from ADGM. |
| UAE | Means the United Arab Emirates. |
| Undertaking | Means:<br>(a) a Body Corporate or Partnership; or<br>(b) an unincorporated association carrying on a trade or business, with or without a view to profit. |
| UN Consolidated List | Means the consolidated list of all individuals and entities subject to measures imposed by the UNSC. |
| unhosted wallet | Has the meaning given in section 10.3. |
| Unlawful Organisation | Means an organisation, the establishment or activities of which have been declared to be criminal under Federal AML Legislation. |
| UNSC | Means the United Nations Security Council. |
| VA/FRT transfer | Has the meaning given in section 10.3. |
| Virtual Asset | Has the meaning given in section 258 of FSMR. |
| Waiver | Means in relation to GEN 8.2, written notice provided under FSMR. |
| WMD | Means weapons of mass destruction. |

## 4. GENERAL COMPLIANCE REQUIREMENTS

### 4.1 General requirements

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;

(d) 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.

(5) The review process may be undertaken:

(a) internally by its internal audit or compliance function; or

(b) by a competent firm of independent auditors or compliance professionals.

4.1.2 (1) The review process required under Rule 4.1.1(4) must cover at least the following:

(a) a sample testing of customer documentation relevant to an assessment of the adequacy of the customer risk assessment or CDD performed by the Relevant Person;

(b) an analysis of all Suspicious Activity/Transaction Reports to highlight any area where procedures or training may need to be enhanced; and

(c) a review of the adequacy of the level of responsibility and oversight of the Relevant Person's Governing Body and Senior Management in ensuring the Relevant Person has implemented and maintained adequate controls.

**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).

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 Groups, branches and subsidiaries

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.

(3) Where the regulator in another jurisdiction does not permit the implementation of policies, procedures, systems and controls consistent with these Rules, the Relevant Person must:

(a) inform the Regulator in writing immediately; and

(b) apply appropriate additional measures to manage the money laundering risks posed by the relevant branch or subsidiary.

**Guidance**

A Relevant Person that is an ADGM Entity should conduct a periodic review to verify that any branch or subsidiary operating in another jurisdiction is in compliance with the obligations imposed under these Rules.

**4.2.2** A Relevant Person must:

(a) communicate the policies and procedures that it establishes and maintains in accordance with these Rules to its Group entities, branches and subsidiaries; and

(b) document the basis for its satisfaction that the requirement in Rule 4.2.1(1) is met.

**Guidance**

In relation to an Authorised Person, if the Regulator is not satisfied with respect to the AML/TFS compliance of its branches and subsidiaries in another jurisdiction, it may take action, including making it a condition of the Authorised Person's Financial Services Permission that it must not operate a branch or subsidiary in that jurisdiction.

## 4.3 Group policies

4.3.1 A Relevant Person which is part of a Group must ensure that it:

(a) has developed and implemented policies and procedures for the sharing of information between Group entities, including the sharing of information relating to CDD and money laundering risks;

(b) has in place adequate safeguards on the confidentiality and use of information exchanged between Group entities, including consideration of relevant data protection legislation;

(c) remains aware of the money laundering risks of the Group as a whole and of its exposure to the Group and takes active steps to mitigate such risks;

(d) contributes to a Group-wide risk assessment to identify and assess money laundering risks for the Group; and

(e) provides its Group-wide compliance, audit and AML/TFS functions with customer account and Transaction information from its Branches and Subsidiaries when necessary for AML/TFS purposes.

## 4.4 Notifications

4.4.1 A Relevant Person must inform the Regulator in writing immediately if, in the course of its activities carried on in or from ADGM or in relation to any of its Branches or Subsidiaries, it:

(a) receives a request for information from a regulator or agency in another jurisdiction responsible for AML/TFS or Sanctions regarding enquiries into potential money laundering;

(b) becomes aware, or has reasonable grounds to believe, that the following has or may have occurred in or through its business:

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

(ii) a breach of Sanctions; or

(iii) acts amounting to bribery under the Organisation for Economic Co-operation and Development ("OECD") Convention on Combatting Bribery of Foreign Public Officials in International Business Transactions;

(c) becomes aware of any money laundering or Sanctions matter in relation to the Relevant Person or a member of its Group which could result in adverse reputational consequences to the Relevant Person; or

(d) becomes aware of a significant breach of a Rule in the AML Rulebook or a breach of relevant Federal AML Legislation.

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. In connection with Rule 4.4.3, 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, electronic copies and certified copies, in respect of the customer business relationship including:

(i) business correspondence and other information relating to a customer's account;

(ii) sufficient records of transactions to enable individual transactions to be reconstructed; and

(iii) internal findings and analysis relating to a transaction or any business if the transaction or business appears unusual or suspicious, whether or not it results in a Suspicious Activity/Transaction Report;

(c) internal notifications of suspicious activity made to its MLRO under Rule 14.2.2;

(d) Suspicious Activity/Transaction Reports and any relevant supporting documents and information, including internal findings and analysis;

(e) any relevant communications with the FIU;

(f) the documents in Rule 4.6.1;

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

(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, 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. 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 records referred to in Rule 4.5.1.

**Guidance**

The Regulator expects that a Relevant Person will be able to ordinarily provide the records within one Business Day of a request from the Regulator.

4.5.3 A Relevant Person must document, and provide to the Regulator immediately any of the following:

(a) the risk assessment of its business as required by Rule 6.1.1;

(b) how the assessment in (a) was used for the purposes of complying with Rule 6.1.2;

(c) the risk assessment of the customer undertaken under Rule 7.1.1(1)(a); and

(d) the determination made under Rule 7.1.1(1)(b).

4.5.4 The records maintained by a Relevant Person must be kept in such a manner that:

(a) the Regulator or another competent third party is able to assess the Relevant Person's compliance with legislation applicable in ADGM;

(b) any Transaction which was processed by or through the Relevant Person on behalf of a customer or other third party can be reconstructed;

(c) any customer or third party can be identified;

(d) all internal notifications of suspicious activity made to its MLRO under Rule 14.2.2, and all SAR/STRs, can be identified; and

(e) the Relevant Person can satisfy, within an appropriate time, any regulatory enquiry or court order to disclose information.

**Guidance**

1. The records required to be kept under Rule 4.5.1 may be kept in electronic format, provided that such records are readily accessible and available to respond promptly to any requests from the Regulator for information.

2. If the date on which the business relationship with a customer ended is unclear, it may be taken to have ended on the date of the completion of the last Transaction.

4.5.5 Where the records referred to in Rule 4.5.1 are kept by a Relevant Person outside ADGM, a Relevant Person must:

(a) take reasonable steps to ensure that the records are held in a manner consistent with these Rules;

(b) ensure that the records are easily accessible to the Relevant Person; and

(c) upon request by the Regulator, ensure that the records are immediately available for inspection.

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 4.5.1 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).

## 4.6 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**

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.

## 4.7 Co-operation with the Regulator

4.7.1 A Relevant Person must:

(a) be open and co-operative in all its dealings with the Regulator; and

(b) ensure that any communication with the Regulator is conducted in the English language.

## 4.8 Employee disclosures

4.8.1 A Relevant Person must 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.

**Guidance**

The Regulator considers that a "relevant body" in Rule 4.8.1 would include the FIU, any other financial intelligence unit, the police, or an Abu Dhabi or Federal ministry or authority.

## 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, where customers are from Jurisdictions Subject to a Call for Action, Enhanced CDD must always be undertaken.

## 5. APPLYING A RISK-BASED APPROACH TO AML/TFS

### 5.1 The risk-based approach

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

(b) ensure that any risk-based assessment undertaken for the purposes of complying with a requirement in the AML Rulebook is:

(i) objective and proportionate to the risks;

(ii) based on reasonable grounds;

(iii) properly documented; and

(iv) updated at appropriate intervals.

**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, a minimum of 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).

5. Section 4.5 sets out the requirements regarding record-keeping for the purposes of the AML Rulebook. These Rules apply in relation to Rule 5.1.1(b)(iii).

## 6. BUSINESS RISK ASSESSMENT

### 6.1 Assessing the money laundering risks of a business

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;

(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 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 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.

6.1.4 Before launching any new product, service, or business practice, 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; 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.

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.

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.

5. A Relevant Person should, as a clearly identifiable element within its overall business risk assessment, undertake a Targeted Financial Sanctions risk assessment to identify, understand, assess and mitigate those risks. This should include conducting a proliferation financing and terrorist financing risk assessment.

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.

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.

8. A business risk assessment 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.

## 7. CUSTOMER RISK ASSESSMENT

### 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).

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

(a) the customer and any Beneficial Owners;

(b) the purpose and intended nature of the business relationship, and the nature of the customer's business;

(c) the nature, ownership and control structure of the customer, its beneficial ownership (if any) and its business;

(d) the customer's country of origin, residence, nationality, place of incorporation or place of business;

(e) the relevant product, service or Transaction;

(f) in relation to life insurance or other similar insurance policies, the beneficiary of the policy and Beneficial Owners of the beneficiary; and

(g) the outcomes of the business risk assessment undertaken under Chapter 6.

**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 (c));

(iii) customer is a Legal Person or a Legal Arrangement that is a vehicle for holding personal assets;

(iv) customer is a company that has nominee shareholders or shares in bearer form;

(v) customer is a business that is cash intensive, such as a business that receives a majority of its revenue in cash;

(vi) corporate structure of the customer or any group to which it belongs is unusual or excessively complex, given the nature of the business;

(b) product, service, transaction or delivery channel risk factors, including whether:

(i) the service involves private banking;

(ii) the product, service or transaction is one that might allow for anonymity or obfuscation of the true identity of any of the parties involved in the transaction;

(iii) the situation involves NFTF business relationships or transactions, or lacks appropriate safeguards, such as electronic signatures or eKYC;

(iv) payments will be received from unknown or unassociated third parties;

(v) the service involves the provision of nominee directors, nominee shareholders or shadow directors or the formation of companies in another country;

(vi) new products and new business practices are involved, including new delivery mechanisms or the use of new or developing technologies for both new and pre-existing products; and

(c) geographical or jurisdictional risk factors, including whether the relevant country or countries:

(i) are identified by credible sources, as:

(A) not having effective systems to counter money laundering; or

(B) not implementing requirements to counter money laundering that are consistent with FATF Recommendations;

(ii) are identified by credible sources as having significant levels of corruption or other criminal activity, such as terrorism, money laundering or the production and supply of illicit drugs;

(iii) are subject to Sanctions, embargos or similar measures issued by, for example, the United Nations or the State;

(iv) are identified by credible sources as providing funding or support for terrorism;

(v) have organisations operating within their territory that have been designated by the State, other countries or International Organisations as terrorist organisations.

(2) Where a customer is a foreign PEP or has a Beneficial Owner that is a foreign PEP, 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 (c));

(iii) an Authorised Person or Recognised Body;

(iv) a Regulated Financial Institution that is subject to regulation and supervision, including AML/TFS regulation and supervision, in a jurisdiction with AML/TFS regulations that are equivalent to the standards set out in the FATF Recommendations;

(v) a Subsidiary of a Regulated Financial Institution referred to in (iv), if the law that applies to the Parent ensures that the Subsidiary also observes the same AML/TFS standards as its Parent;

(vi) a company whose Securities are listed by the Regulator, a Non-ADGM Financial Services Regulator or a Regulated Exchange, which is subject to disclosure obligations broadly equivalent to those set out in the Market Rules;

(vii) a law firm, notary firm or other legal business that carries on its business in ADGM;

(viii) an accounting firm, insolvency firm, auditor or other audit firm that carries on its business in ADGM;

(b) product, service, transaction or delivery channel risk factors, including whether the product or service is:

(i) a Contract of Insurance which is non-life insurance;

(ii) a Contract of Insurance which is a life insurance product with no investment return or redemption or surrender value;

(iii) an insurance policy for a pension scheme that does not provide for an early surrender option, and cannot be used as collateral;

(iv) a pension, superannuation or similar scheme that satisfies the following conditions:

(A) the scheme provides retirement benefits to employees;

(B) contributions to the scheme are made by way of deductions from wages; and

(C) the scheme rules do not permit the assignment of a member's interest under the scheme;

(v) a product where the risks of money laundering are adequately managed by other factors such as transaction limits or transparency of ownership; and

(c) geographical and jurisdictional risk factors, including whether a country or countries:

(i) are identified by credible sources as having effective systems to counter money laundering;

(ii) are identified by credible sources as having a low level of corruption or other criminal activity, such as terrorism, money laundering, or the production and supply of illicit drugs;

(iii) have been assessed by credible sources, as having:

(A) requirements to counter money laundering that are consistent with the FATF Recommendations; and

(B) effectively implement FATF Recommendations.

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 what 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, a Relevant Person is required to carry out Enhanced CDD under Rule 8.4, 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 all other 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.

**Guidance on high-risk customers**

1. When assessing the risk factors referred to in 7.1.2(1), the presence of one or

more risk factors may not always indicate a high risk of money laundering in a particular situation.

2. An example of a business relationship conducted in unusual circumstances, for the purposes of Rule 7.1.2(1)(a)(i), would include, but is not limited to a business relationship or proposed business relationship that involves, or would involve, significant unexplained geographic distance between the location of the Relevant Person and the customer or proposed customer.

3. The highest risk products or services in respect of money laundering are those where unlimited third-party funds can be freely received from or paid to third parties, without evidence of the identity of the third parties being obtained and the identity being verified.

4. Money laundering risks are likely to be increased if a Person is able to hide behind corporate structures such as limited companies, trusts, special purpose vehicles and nominee arrangements. When devising its internal procedures, a Relevant Person should consider how its customers and operational systems impact the capacity of its staff to identify suspicious activities and Transactions. Generally, the lowest risk products in respect of money laundering are those where funds can only be received from a named customer by way of payment from an account held in the customer's name, and similarly where the funds can only be remitted to a named customer.

**Guidance on low-risk customers**

When assessing the risk factors referred to in 7.1.3(1), a Relevant Person must bear in mind that the presence or absence of one or more risk factors may not always indicate a high or low risk of money laundering, respectively, in a particular situation.

## 7.2 Prohibition on establishing business relationships with certain customers

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 prevent the Relevant Person from identifying one or more of the customer's Beneficial Owners.

7.2.2 A Relevant Person must not establish or maintain a business relationship with a Shell Bank.

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 Relevant Person should not permit a customer to use the Relevant Person's products and services to engage in business with a Shell Bank.

7.2.4 If a Relevant Person uses a numbered account with an abbreviated name, it must ensure that:

(a) such an account is used only for internal purposes;

(b) it has undertaken the same CDD procedures in relation to the account holder as are required for other account holders;

(c) it maintains the same information in relation to the account and account holder as is required for other accounts and account holders; and

(d) staff performing AML/TFS functions, including staff responsible for identifying and monitoring transactions for suspicious activity, and staff performing compliance and audit functions, have full access to information about the account and the account holder.

**Guidance on anonymous accounts**

A Relevant Person should note that, in addition to the prohibition in Rule 7.2.3 against knowingly establishing anonymous accounts, accounts in a fictitious name or nominee accounts, Federal AML Legislation also prohibits the opening of accounts held under borrowed, mock or fake names or accounts designated solely with numbers and without the names of account holders.

**Guidance on Restricted Scope Companies**

1. A Restricted Scope Company is a corporate vehicle offering a greater degree of confidentiality than other forms of corporate entity in ADGM. Restricted Scope Companies are not required to file accounts and are not required to have their accounts audited. Restricted Scope Companies must file an annual return, articles, and details of their registered offices, directors and secretary (if they have one) with the ADGM Registrar of Companies.

2. Relevant Persons will know that Restricted Scope Companies are subject to less onerous corporate disclosure requirements than other forms of corporate entities due to the requirement to have "(Restricted)" in a company's name. Given that only the constitution and details of the registered office of a Restricted Scope Company will be available in a public register, a Relevant Person will be required to have a bilateral dialogue with the Restricted Scope Company, in accordance with the RBA, to obtain any other relevant information which it needs to assess the money laundering risks to which it is exposed.

3. Restricted Scope Companies should be forthcoming with relevant information in response to requests by other Persons and entities for the purpose of compliance of the latter with the requirements in the AML Rulebook. The fact that Restricted Scope Companies are not subject to strict standards of disclosure of corporate documentation to a public registry should not be interpreted by Restricted Scope

Companies to limit or prohibit their providing of any relevant information to other Persons and entities for AML/TFS purposes.

## 8. CUSTOMER DUE DILIGENCE

### 8.1 Requirement to undertake Customer Due Diligence

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, or several 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, or several 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

(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.

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. A PFP Prospect is a customer for the purposes of the AML Rulebook, and a Relevant Person that is a PFP Operator should undertake CDD as part of due diligence performed pursuant to COBS 18.4.1.

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

7. 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;

      (iii) the payment for any part or all of the sale/purchase amount includes funds that were converted from or to a 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 A Relevant Person must undertake CDD as required by Rule 8.1.1 at the following times (as applicable):

(a) when it is establishing the relevant business relationship with the customer;

(b) before carrying out the relevant Transaction or services; or

(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 (1) A Relevant Person 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:

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

(b) deferral of verification is necessary in order not to interrupt the normal course of business; and

(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).

(2) Where a Relevant Person, having relied on Rule 8.2.1, 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 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:

(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 services, excluding any reasonable costs incurred by the Relevant Person; or

(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

(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.

8.2.3 A Relevant Person must ensure that its AML/TFS systems and controls referred to in Rule 4.1.1 include risk management policies and procedures concerning the conditions under which business relationships may be established, 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 SAR/STRs and tipping off.

## 8.3 Standard Customer Due Diligence requirements

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

(a) identify the customer and verify the customer's identity including identification and verification of the identity of any Person purporting to act on behalf of the customer;

(b) identify all the Beneficial Owners and take reasonable measures to verify the identity of the Beneficial Owners, such that the Relevant Person is satisfied that it knows who the Beneficial Owners are;

(c) assess and understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship; and

(d) conduct ongoing due diligence of the business relationship as required under Rule 8.6.1.

(2) In addition to complying with (a), for life insurance or other similar policies a Relevant Person must:

(a) record the names of any beneficiaries named in the policy;

(b) verify the identity of all Persons in all classes of beneficiaries when a payout of the policy is due;

(c) undertake the measures referred to in (a) and (b) as soon as the beneficiary of the policy is identified or designated; and

(d) verify the identity of beneficiaries and any Beneficial Owners of a beneficiary before it makes a payout under the policy.

(3) A Relevant Person must have systems and controls in place and take reasonable measures to determine whether:

(a) a customer;

(b) any Beneficial Owners of the customer; or

(c) for a life insurance or other similar policy, any beneficiary of the policy, or any Beneficial Owners of a beneficiary,

is a PEP.

(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;

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

(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 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.

(4) If a customer is a foundation, the Relevant Person must obtain and verify:

(a) a certified copy of the charter and by-laws of the foundation or any other documents constituting the foundation; and

(b) documentary evidence of the appointment of the guardian or any other person who may exercise powers in respect of the foundation.

(5) If a customer is a trust or other similar Legal Arrangement, the Relevant Person must obtain and verify:

(a) a certified copy of the trust deed or other documents that set out the nature, purpose and terms of the trust or arrangement; and

(b) documentary evidence of the appointment of the trustee or any other person exercising powers under the trust or arrangement.

**Guidance**

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 reassess the customer's risk classification and the associated level of due diligence to be undertaken.

4. For residents of the UAE, the UAE Pass may be used to identify and verify the identity of a customer who is a Natural Person, and thereby satisfy the requirement to verify the address of that customer only where the UAE Pass is duly authenticated by the Relevant Person.

5. The Relevant Person must always verify the address of a customer subject to Enhanced Customer Due Diligence under Rule 8.4.1.

6. Where personal identity documents, such as a passport, identity card or other identification documentation cannot be reviewed in original form, the identification documentation provided should be certified as a true copy of the original document by any one of the following:

   (a) a registered lawyer;

   (b) a registered notary;

   (c) a chartered accountant;

   (d) a government ministry;

   (e) a post office;

   (f) a police officer; or

   (g) an embassy or consulate.

The individual or authority undertaking the certification should be contactable if necessary. Where a copy of an original identification document is made by a Relevant Person, the copy should be dated, signed and marked with 'original sighted'.

7. In complying with Rule 8.3.2(2), a Relevant Person should take reasonable steps to identify whether a customer has more than one nationality or residency rights in jurisdictions other than their jurisdiction of birth. The existence of such residency rights or dual nationality may be a potential risk factor and should be considered as such in the customer risk assessment required by Rule 7.1.1(3) and Rule 7.1.2.

8. Where a Relevant Person uses eKYC for CDD purposes appropriate measures must be adopted to mitigate the risks that may arise from eKYC processes and the use of an eKYC System. A Relevant Person must ensure that eKYC is secure and effective, includes an appropriate combination of authentication factors when verifying the identity of the customer and ensure it is at least as stringent as face-to-face CDD. Measures should be in place to verify the authenticity of any official government identification document and the actual customer. A Relevant Person should also apply guidance on technical standards for biometric authentication issued by the Regulator or a competent authority of the UAE, as applicable.

9. When employing an eKYC System to assist with CDD, a Relevant Person should:

   a. ensure that it has a thorough understanding of the eKYC System itself and the risks of eKYC, including those outlined by relevant guidance from FATF and other international standard setting bodies;

   b. comply with all the Rules of the Regulator relevant to eKYC, including, but not limited to, applicable requirements regarding the business risk assessment, as per Rule 6.1, and outsourcing, as per Rule 9.3;

   c. combine eKYC with transaction monitoring, anti-fraud and cyber-security measures to support a wider framework preventing applicable Financial Crime; and

   d. take appropriate steps to identify, assess and mitigate the risk of the eKYC system being misused for the purposes of Financial Crime.

10. In undertaking CDD, a Relevant Person that is a Recognised Body should have regard to the provisions of 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.

(2) The Relevant Person must identify any Natural Person who:

(a) owns or controls (in each case whether directly or indirectly) 25% or more of the shares or voting rights in the Body Corporate;

(b) controls the Body Corporate; or

(c) exercises ultimate control over the management of the Body Corporate.

(3) For the purposes of (2)(b), a Natural Person controls a Body Corporate if such person:

(a) holds, directly or indirectly:

(i) 25% or more of the Body Corporate's shares;

(ii) 25% or more of the voting rights in the Body Corporate; or

(iii) the right to appoint or remove a majority of the board of directors of the Body Corporate; or

(b) has the right to exercise, or actually exercises, significant influence or control over the Body Corporate.

(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).

(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.

8.3.4 (1) For the purposes of Rule 8.3.1(1)(b), a Relevant Person must identify the Beneficial Owners of a Partnership in accordance with this Rule.

(2) The Relevant Person must identify any Natural Person who:

(a) ultimately is entitled to or controls (in each case whether directly or indirectly) a 25% or more share of the capital or profits of the Partnership or 25% or more of the voting rights in the Partnership; or

(b) otherwise exercises ultimate control over the management of the Partnership.

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.

(2) The Relevant Person must identify:

(a) the settlor of the trust;

(b) any other trustee(s) aside from the customer;

(c) each beneficiary of the trust;

(d) where the persons or some of the persons benefiting from the trust have not been determined, the class of persons in whose main interest, in the opinion of the Registrar, the trust has been established or operates; and

(e) any Natural Person who has control over the trust.

(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 (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.

(2) The Relevant Person must identify:

(a) the founder;

(b) the foundation council members, or otherwise members of the governing body of the foundation;

(c) the guardian, if any;

(d) the beneficiaries, if named, or designee if no beneficiaries are named, in whose main interest, in the opinion of the Relevant Person, the foundation or arrangement has been established or operates; and

(e) any Natural Person who has control over the foundation or other Legal Arrangement.

(3) For the purposes of (2)(e), a Natural Person shall have "control" over a foundation or a Legal Arrangement if such person:

(a) holds, directly or indirectly, 25% or more of the voting rights in the conduct and management of the foundation or the Legal Arrangement; or

(b) holds the right, directly or indirectly, to appoint or remove a majority of the officials of the foundation or the Legal Arrangement.

(4) Where any of the persons identified under (2)(a) to (d) are 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.

**Guidance**

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.

2. For a retail investment fund that is widely-held and where the investors invest via pension contributions, the Regulator would not expect the manager of the fund to look through to any underlying investors where there are none with any material control or ownership of the fund. However, for a closely-held fund with a small number of investors, each having a large shareholding or other interest, the Regulator would expect a Relevant Person to identify and verify each of the Beneficial Owners, depending on the risks identified as part of its risk-based assessment of the customer. For a corporate health policy with defined benefits, however, the Regulator would not expect a Relevant Person to identify the Beneficial Owners.

3. An eKYC System may be used as part of the identification and verification of Beneficial Owners. When determining whether to use an eKYC System to assist in the CDD of a Beneficial Owner, a Relevant Person should establish if the eKYC System used allows it to comply fully with the relevant Rules in relation to CDD.

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. Identifying and recording the relevant Natural Person(s) for the purposes of Rule 8.3.3(4) does not determine the customer risk assessment. In such cases, the customer risk assessment should continue to reflect the actual risk profile of the customer.

## 8.4 Enhanced Customer Due Diligence

8.4.1 (1) A Relevant Person must undertake Enhanced CDD on a customer:

(a) that is assigned a high-risk rating;

(b) from a Jurisdiction Subject to a Call for Action; and

(c) before sending or receiving a VA/FRT transfer to or from an unhosted wallet for that customer under Rule 10.3.6(1).

(2) A Relevant Person must undertake Enhanced CDD in addition to CDD under Rule 8.3.1as 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;

(b) update the CDD information which it holds on the customer and any Beneficial Owners more regularly;

(c) identify and verify:

(i) the Source of Funds; and

(ii) the Source of Wealth;

of the customer and, if applicable, all Beneficial Owners;

(d) conduct enhanced monitoring of the business relationship, by increasing the frequency and intensity of controls applied, and determining which groups of transactions need further examination;

(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.

**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 or by a committee 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.

3. For high-risk customers, a Relevant Person should, in order to mitigate the perceived potential and actual risks, exercise a greater degree of diligence throughout the course of the customer relationship and should endeavour to understand the nature of the customer's business and consider whether it is consistent and reasonable.

4. A Relevant Person should be satisfied that a customer's use of complex legal structures and/or the use of trust and private investment vehicles, has a genuine and legitimate purpose.

5. For Enhanced CDD, where there are one or more Beneficial Owners, verification of the customer's Source of Funds and Wealth may require enquiring into the Beneficial Owners' Source of Funds and Wealth because the Source of the Funds would normally be associated with the Beneficial Owners and not the customer.

6. The Regulator considers that verification of Source of Funds includes obtaining independent corroborating evidence such as the proof of dividend payments connected to a shareholding, bank statements, salary/bonus certificates, loan documentation and proof of all Transactions which gave rise to payments into the account. A customer should be able to demonstrate and have documented how the relevant funds are connected to a particular event which gave rise to the payment into the account or to the source of the funds for a Transaction.

7. The Regulator considers that verification of Source of Wealth includes obtaining independent corroborating evidence such as share certificates, publicly available registers of ownership, bank or brokerage account statements, probate documents, audited accounts and financial statements, news items from a reputable source and other similar evidence.

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.

## 8.5 Simplified Customer Due Diligence

8.5.1 (1) Where a Relevant Person is permitted to undertake Simplified CDD under Rule 8.1.1(4), modification of Rule 8.3.1 may include:

(a) verifying the identity of the customer and any Beneficial Owners after the establishment of the business relationship;

(b) deciding to reduce the frequency of, or as appropriate not undertake, customer identification updates;

(c) deciding not to verify an identification document other than by requesting a copy;

(d) reducing the degree of ongoing monitoring of Transactions, based on a reasonable monetary threshold or on the nature of the Transaction; and

(e) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring such purpose and nature from the type of Transactions or business relationship established.

(2) The modification undertaken under (1) must be proportionate to the customer's money laundering risks.

**Guidance**

1. A Relevant Person should not use a "one size fits all" approach for all of its low-risk customers. Notwithstanding that the risks may be low for all such customers in that

category, the extent of CDD undertaken needs to be proportionate to the specific risks identified on a case-by-case basis.

2. A Relevant Person might reasonably reduce the frequency of or, as appropriate, eliminate customer identification updates where the money laundering risks are low and the service provided does not offer a realistic opportunity for money laundering.

3. An example of where a Relevant Person might reasonably reduce the degree of ongoing monitoring and scrutinising of Transactions, based on a reasonable monetary threshold or on the nature of the Transaction, would be where the Transaction is a recurring, fixed contribution to a savings scheme, investment portfolio or fund or where the monetary value of the Transaction is not material for money laundering purposes given the nature of the customer and the Transaction type.

## 8.6 Ongoing Customer Due Diligence

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, their business and risk rating;

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

(c) enquire into the background and purpose of the Transactions in (b);

(d) periodically review the adequacy of the CDD information it holds on customers and Beneficial Owners to ensure that the information is kept up to date, particularly for customers with a high-risk rating; and

(e) periodically review each customer to ensure that the risk rating assigned to a customer under Rule 7.1.1(1)(b) remains appropriate for the customer in light of the money laundering risks.

8.6.2 A Relevant Person must apply an intensified and ongoing monitoring programme with respect to higher risk Transactions and customers.

**Guidance**

1. The customer identification process does not end at the time of establishing a business relationship with a customer or, where relevant, undertaking a specific transaction or business activity on behalf of a customer. Following the start of the customer relationship, a Relevant Person should ensure that all relevant evidence and information is kept up to date including, for example, the list of authorised signatories who can act on behalf of a corporate customer.

2. In complying with Rule 8.6.1(d), a Relevant Person should undertake a periodic review to ensure that non-static customer identity documentation is accurate and up to date. A Relevant Person is expected to ensure that the information and the evidence obtained from a customer is valid and has not expired, for example, when obtaining copies of identification documentation such as a passport or identification card. Examples of non-static identity documentation include passport number and residential/business address and, for a Legal Person, its share register or list of partners.

3. A Relevant Person should undertake a review under Rule 8.6.1(d) and (e) particularly when:

   (a) the Relevant Person changes its CDD documentation requirements;

   (b) an unusual Transaction with the customer is expected to take place;

   (c) there is a material change in the business relationship with the customer; or

   (d) there is a material change in the nature or ownership of the customer.

4. The degree of the ongoing due diligence to be undertaken will depend on the customer risk assessment carried out under Rule 7.1.1.

5. A Relevant Person's Transaction monitoring policies, procedures, systems and controls, which may be implemented by manual or automated systems, or a combination thereof, are one of the most important aspects of effective CDD. Whether a Relevant Person should undertake the monitoring by means of a manual or computerised system, or both, will depend on a number of factors, including:

   (a) the size and nature of the Relevant Person's business and customer base; and

   (b) the complexity and volume of customer Transactions.

8.6.3 A Relevant Person must review its customers, their businesses, and Transactions, against Sanctions Lists when complying with Rule 8.6.1(d).

## 8.7 Failure to conduct or complete Customer Due Diligence

8.7.1 (1) Where, in relation to a customer, a Relevant Person is unable to conduct or complete the requisite CDD in accordance with Rule 8.1.1 it must, where appropriate:

   (a) not carry out a Transaction with or for the customer through a bank account or in cash;

   (b) not open an account or otherwise provide a service;

   (c) not otherwise establish a business relationship or carry out a Transaction;

(d) terminate or suspend any existing business relationship with the customer;

(e) return any monies or assets received from the customer; and

(f) consider whether the inability to conduct or complete CDD necessitates the making of a Suspicious Activity/Transaction Report under Rule 14.3.1(c).

(2) A Relevant Person is not obliged to comply with (1)(a) to (e) if:

(a) to do so would amount to "tipping off" the customer, in breach of Federal AML Legislation; or

(b) the FIU directs the Relevant Person to act otherwise.

**Guidance**

1. In complying with Rule 8.7.1(1) a Relevant Person should apply one or more of the measures in (a) to (f) as appropriate in the circumstances. Where CDD cannot be completed to a significant degree, it may be appropriate not to carry out a Transaction pending completion of CDD. Where CDD cannot be conducted, including where a material part of the CDD such as identifying and verifying Beneficial Owners cannot be undertaken, a Relevant Person should not establish a business relationship with the customer.

2. A Relevant Person should note that Rule 8.7.1 applies to both existing and prospective customers. For prospective customers it may be appropriate for a Relevant Person to terminate the business relationship before a product or service is provided. However, for existing customers, while termination of the business relationship should not be ruled out, suspension may be more appropriate depending on the circumstances, whilst further investigations are carried out. Whichever course of action is taken, the Relevant Person should be careful not to tip off the customer.

3. A Relevant Person should adopt the RBA in order to inform the appropriate level of CDD to be undertaken for existing customers. For example, if a Relevant Person considers that any of its existing customers (which may include customers that it migrates into ADGM) have not been subject to CDD of a standard equivalent to that required by the AML Rulebook, it should adopt the RBA and take remedial action in a manner proportionate to the risks and within a reasonable period of time whilst complying with Rule 8.7.

## 8.8 Portability of Customer Due Diligence information

8.8.1 (1) A Relevant Person "A" that is an Authorised Person or a Recognised Body must provide another Relevant Person, "B", that is an Authorised Person or a Recognised Body, at the request of B, with the Customer Due Diligence information for customers that has been collected by A under Rules 8.3 and 8.4, subject to:

(a) those customers being customers of both A and B at the time that the request is made;

(b) B obtaining the written consent of the customers to whom the request relates and providing A with that consent for the release of such information by A;

(c) the request being made solely for the purposes of conducting Customer Due Diligence on the customers to whom the request relates; and

(d) in the preceding twelve months B not having requested Customer Due Diligence information from A for the same customers to whom the request relates.

(2) Relevant Person A must also provide Relevant Person B with any other information relevant to CDD that has been provided to it by those customers.

8.8.2 Following a request made under Rule 8.8.1, A must transfer to B without undue delay all Customer Due Diligence information in its possession for those customers.

8.8.3 Relevant Person A must not charge B a fee for the provision of Customer Due Diligence information provided under Rule 8.8.1.

## 9. THIRD PARTY CDD, BUSINESS PARTNER DUE DILIGENCE AND OUTSOURCING ELEMENTS OF CDD

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

9.1.1 (1) Subject to (2), a Relevant Person may rely on the following 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.

(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.

(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.

(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:

(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 (3), the information is up to date.

(5) Where a Relevant Person relies on a member of its Group, such Group member need not meet the condition in (4)(c) if:

(a) the Group applies and implements Group-wide policies on AML/TFS compliance that meet the standards set out in the FATF Recommendations; and

(b) the Group is supervised for compliance with those policies by a Non-ADGM Financial Services Regulator in a country with AML/TFS requirements equivalent to the standards set out in the FATF Recommendations.

(6) If a Relevant Person is not reasonably satisfied that a customer or Beneficial 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.

(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 of, Anti-Money Laundering Legislation.

9.1.2 (1) When assessing under Rule 9.1.1(4) or (5) if AML/TFS requirements in another jurisdiction are equivalent to the standards set out in the FATF Recommendations, a Relevant Person must take into account factors including:

(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 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(4)(a), "immediately obtaining the necessary CDD information" means obtaining all relevant CDD information, and not just basic information such as name and address. Compliance can be achieved by sending the information via email or another appropriate means. A Relevant Person is not required to immediately obtain the underlying certified documents used by the third party to undertake its CDD. However, pursuant to Rule 9.1.1(4)(b), these must be available on request without delay.

2. The Regulator would expect a Relevant Person, in complying with Rule 9.1.1(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(4)(b), the Relevant Person should undertake the relevant CDD itself and should not seek to rely on the relevant third party.

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 Know your business partner

9.2.1 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.

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.

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**

1. A 'business partner' may include:

   a. any of the Persons specified in Rule 9.1.1(1);

   b. a service provider performing elements of CDD for a Relevant Provider, pursuant to Rule 9.3.1; and

   c. other service providers.

   Service providers include agents that directly facilitate the activities of Relevant Persons in servicing their clients, as distinct from service providers that provide purely ancillary services, such as software or facilities management, where the money laundering risks of the relationship to a Relevant Person are low.

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

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.

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.

### 9.3 Outsourcing elements of CDD

9.3.1 A Relevant Person which outsources any element of its CDD to a service provider, including a service provider within its Group, remains responsible for compliance with, and liable for any failure to meet the requirements of, Anti-Money Laundering Legislation.

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.

9.3.4 After engaging a service provider, a Relevant Person must undertake periodic assurance assessments to ensure that the services comply with the agreement and allow 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.

2. Outsourcing elements of CDD includes using digital identity verification services, screening services and using a service provider's eKYC System for Section 9.3.

3. When undertaking an assessment of an eKYC System for Rule 9.3.3(3), a Relevant Person should consider relevant assurance standards issued by competent authorities and standard-setting bodies.

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.

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, 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.

6. A Relevant Person should ensure that the service provider can be replaced with minimal disruption if the outsourcing arrangement is terminated.

9.3.5 Authorised Persons Providing Money Services

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

   (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;

   (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;

   (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;

   (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

   (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, ELECTRONIC FUND TRANSFERS, VIRTUAL ASSETS AND FIAT-REFERENCED TOKENS TRANSFERS AND THE TRAVEL RULE, AUDIT AND ANONYMOUS ACCOUNTS

## 10.1 Correspondent Banking

10.1.1 An Authorised Person proposing to enter into a Correspondent Banking relationship must:

(a) undertake appropriate CDD on the Respondent Bank;

(b) as part of (a), gather sufficient information about the Respondent Bank to fully understand the nature of 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 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 AML/TFS controls and ascertain where they are adequate and effective in light of the FATF Recommendations;

(e) obtain prior approval from Senior Management before establishing the Correspondent Banking relationship;

(f) ensure that the respective responsibilities of the Correspondent Bank and Respondent Bank are clearly understood and properly documented;

(g) be satisfied that, in relation to any customers of the Respondent Bank that will have direct access to 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 Correspondent Bank upon request; and

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

10.1.2 An Authorised Person must:

(a) not enter into a 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 correspondent banking relationship with, a 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.

2. 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.

## 10.2 Electronic fund transfers and the travel rule

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) a transfer and settlement between Financial Institutions where both the originator and the beneficiary are Financial Institutions acting on their own behalf.

10.2.2 Definitions

(1) In this section 10.2:

(a) "**batch transfer**" means a transfer comprised of multiple individual fund transfers from a single originator that are bundled for transmission,

whether or not the individual fund transfers are ultimately intended for one or more beneficiaries;

(b) "**beneficiary**" means the Person identified by the originator as the recipient of the requested 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;

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

(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.

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

(a) ensure that a fund transfer and any related messages contain the information required by (2) when sending or receiving a fund transfer;

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

(c) monitor fund transfers for the purposes of detecting those 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 or accept fund transfers without the information required under (2) and (3).

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

(a) the full name of the originator;

(b) the originator account number where that account is used to process the fund transfer, or a unique reference number 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

(iv) the 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 fund transfer or a unique reference number where no beneficiary account number exists.

(3) Before effecting a fund transfer, an Authorised Person or Recognised Body that is an originating institution must:

(a) verify the originator information that will accompany the fund transfer under (2);

(b) ensure that for batch transfers, the batch file contains the information set out in (2) and that the beneficiary information included is fully traceable in 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. Authorised Persons and Recognised Bodies should monitor for, and conduct enhanced scrutiny of, suspicious activities, including incoming fund transfers that do not contain complete originator information.

2. The Regulator considers that concealing or removing any of the information required by Rule 10.2.3(2) in a fund transfer would be a breach of 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 Authorised Persons and Recognised Bodies to be aware of and comply with FATF Recommendation number 15, FATF's Interpretative Note (R.15/INR.15) and FATF Recommendation number 16.

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.

## 10.4 Audit

10.4.1 An Authorised Person or a Recognised Body must ensure that its internal audit function undertakes regular reviews and assessments of the effectiveness of the Authorised Person or Recognised Body's money laundering policies, procedures, systems and controls, and its compliance with its obligations in the AML Rulebook.

**Guidance**

1. The review and assessment undertaken for the purposes of Rule 10.4.1 may be undertaken:

(a) internally by the Authorised Person or Recognised Body's internal audit function; or

(b) by a competent firm of independent, external auditors or compliance professionals.

2. The review and assessment undertaken for the purposes of Rule 10.4.1 should cover at least the following:

(a) sample testing of compliance with the Authorised Person or the Recognised Body's CDD arrangements;

(b) an analysis of all notifications made to the MLRO to highlight any area where procedures or training may need to be enhanced; and

(c) a review of the nature and frequency of the dialogue between Senior Management and the MLRO.

### 10.5 Anonymous and nominee accounts

10.5.1 An Authorised Person or a Recognised Body must not establish or maintain:

(a) an anonymous account or an account in a fictitious name; or

(b) a nominee account which is held in the name of one Person, but which is controlled by or held for the benefit of another Person whose identity has not been disclosed to the Authorised Person or the Recognised Body.

## 11. TARGETED FINANCIAL SANCTIONS AND OTHER INTERNATIONAL OBLIGATIONS

### 11.1 Resolutions and Sanctions

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.

(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.

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

(a) a description of the relevant activity in (3)(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.

2. Relevant resolutions or Sanctions mentioned in Rule 11.1.1 may, among other things, relate to money laundering, terrorist financing or the financing of WMD, or otherwise be relevant to the activities carried on by the Relevant Person. For example:

(a) a Relevant Person should exercise due care to ensure that it does not provide services to, or otherwise conduct business with, a Person engaged in money laundering, terrorist financing or the financing of WMD; and

(b) a Recognised Investment Exchange or Recognised Clearing House, as a Recognised Body, should additionally exercise due care to ensure that it does not facilitate fund raising activities or listings by Persons engaged in money laundering or terrorist financing or financing of WMD.

3. A Relevant Person should be proactive in checking for, and taking measures to comply with, relevant resolutions or Sanctions which the Relevant Person is required to comply with, under legislation applicable in ADGM or any other jurisdiction. This should include measures that enable a Relevant Person to comply with their obligations under Federal AML Legislation. The Regulator expects Relevant Persons to perform checks on an ongoing basis against their customer databases and records for any names appearing in resolutions or Sanctions which the Relevant Person is required to comply with as well as to monitor transactions accordingly.

4. A Relevant Person may use a database maintained elsewhere for an up-to-date list of resolutions and Sanctions, or to perform checks of customers or transactions against that list. For example, it may wish to use a database maintained by its head office or a Group member. However, the Relevant Person retains responsibility for ensuring that its systems and controls are effective to ensure compliance with this Rulebook.

5. The requirements of Article 21 of Cabinet Resolution No. (74) of 2020 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 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 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 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 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) the Regulator; and

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

concerning the matters in (2).

(2) For the purposes of (1), the relevant matters are:

(a) arrangements for preventing money laundering, terrorist financing or the financing of weapons of mass destruction in a particular country or jurisdiction, including any assessment of material deficiency in adopting international standards against a relevant country or jurisdiction; and

(b) the names of Persons, groups, organisations or entities or any other body where suspicion of money laundering exists.

(3) For the purposes of (1), measures that a Relevant Person must undertake when taking reasonable measures to comply with findings, recommendations, guidance, directives, resolutions, Sanctions, notices or other conclusions, include, but are not limited to, countermeasures:

(a) requiring specific elements of enhanced CDD;

(b) requiring enhanced reporting mechanisms or systematic reporting of financial transactions;

(c) limiting business relationships or financial transactions with specified persons or persons in a specified jurisdiction;

(d) prohibiting Relevant Persons from relying on third parties located in a specified jurisdiction to conduct CDD;

(e) requiring the review and amendment or, if necessary, termination of correspondent relationships with banks in a specified jurisdiction;

(f) prohibiting the execution of specified electronic fund transfers; or

(g) requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in a specified jurisdiction.

(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 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. 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. Transactions with counterparties located in countries or jurisdictions that were previously, but are no longer, identified as deficient or have been relieved from special scrutiny may nevertheless require attention which is higher than normal.

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.

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.

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.

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.

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.

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.

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. MONEY LAUNDERING REPORTING OFFICER

### 12.1 Appointment of an MLRO

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 12.1.6 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.

**Guidance**

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

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.

12.1.4 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 their absence.

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.

12.1.6 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 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 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 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 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;

(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.

## 12.4 Reporting

12.4.1 The MLRO must report semi-annually to the Governing Body or Senior Management of the Relevant Person on the following matters:

(a) the results of the review under Rule 4.1.1(4);

(b) the Relevant Person's compliance with Federal AML Legislation and the Regulations and Rules of the Regulator (including this AML Rulebook);

(c) relevant findings, recommendations, guidance, directives, resolutions, Sanctions, notices or other conclusions and how the Relevant Person has taken them into account;

(d) internal notification(s) of suspicious activity to the MLRO made under Rule 14.2.2 by the Relevant Person's Employees, or its agents or members of its Group where acting on its behalf, and action taken in respect of those reports, including the grounds for all decisions;

(e) Suspicious Activity/Transaction Reports made by the Relevant Person, or its agents or members of its Group where acting on its behalf, and action taken in respect of those reports, including the grounds for all decisions; and

(f) other relevant matters related to AML/TFS as it concerns the Relevant Person's business.

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 (a) and the action taken pursuant to (b).

12.4.3 The Relevant Person must provide to the Regulator a copy of:

(a) the report provided under Rule 12.4.1; and

(b) the record made under Rule 12.4.2(c).

## 13. AML/TFS TRAINING AND AWARENESS

### 13.1 Training and awareness

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 their deputy;

(ii) understand the relevant legislation relating to money laundering, including Federal AML Legislation;

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

(iv) recognise and deal with Transactions, risks, trends, techniques and other activities which may be related to money laundering;

(v) understand the types of activity that may constitute suspicious activity in the context of the business in which an Employee is engaged and that may warrant an internal notification of suspicious activity to the MLRO under Rule 14.2.2;

(vi) understand its arrangements regarding the making of an internal notification to the MLRO of suspicious activity under Rule 14.2.2;

(vii) be aware of the prevailing techniques, methods and trends in money laundering relevant to the business of the Relevant Person;

(viii) understand the roles and responsibilities of Employees in combatting money laundering; and

(ix) understand the relevant findings, recommendations, guidance, directives, resolutions, Sanctions, notices or other conclusions described in Chapter 11;

(c) ensure that its AML/TFS training:

(i) is appropriately tailored to the Relevant Person's activities, including its products, services, customers, distribution channels, business partners and the level and complexity of its Transactions; and

(ii) indicates the different levels of money laundering risks and vulnerabilities associated with the matters in (i); and

(d) ensure that its AML/TFS training is up to date with money laundering trends and techniques.

### 13.2 Frequency

13.2.1 A Relevant Person must provide AML/TFS training for all Employees in accordance with Rule 13.1.1 at least annually.

### 13.3 Record-keeping

13.3.1 All relevant details of the Relevant Person's AML/TFS training must be recorded, including:

(a) dates when the training was given;

(b) the nature of the training; and

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

13.3.2 These records must be kept for at least six years from the date on which the training was given.

**Guidance**

1. The Regulator considers it appropriate that all new relevant Employees of a Relevant Person be given appropriate AML/TFS training as soon as reasonably practicable after commencing employment with the Relevant Person, and thereafter on a periodic basis.

2. A relevant Employee would include a member of the Senior Management or operational staff, any Employee with customer contact or who handles or may handle customer monies or assets, and any other Employee who might otherwise encounter money laundering in the business.

3. Relevant Persons should take an RBA to AML/TFS training. The Regulator considers that AML/TFS training should be provided by a Relevant Person to each of its relevant Employees at intervals appropriate to the role and responsibilities of the Employee. In the case of an Authorised Person the Regulator expects that training should be provided to each relevant Employee at least annually.

4. The manner in which AML/TFS training is provided by a Relevant Person need not be in a formal classroom setting, rather it may be via an online course or any other similarly appropriate manner.

## 14. SUSPICIOUS ACTIVITY/TRANSACTION REPORTS

### 14.1 Application and definitions

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

### 14.2 Internal reporting requirements

14.2.1 A Relevant Person must establish and maintain policies, procedures, systems and controls in order to monitor and detect suspicious activity or Transactions in relation to potential money laundering or terrorist financing.

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 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.

2. CDD measures form the basis for recognising suspicious activity or Transactions. Sufficient guidance must therefore be given to the Relevant Person's Employees to enable them to form a suspicion or to recognise when they have reasonable grounds to suspect that money laundering or terrorist financing is taking place. This should involve training that will enable relevant Employees to seek and assess the information that is required for them to judge whether a Person is involved in suspicious activity or Transactions related to money laundering or terrorist financing.

3. Where appropriate, a Relevant Person should also utilise the methods described in 1. 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.

4. The requirement for Employees to notify the Relevant Person's MLRO should include situations when no business relationship was developed because the circumstances were suspicious.

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 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 their line manager or other Employees, the responsibility remains with the Employee to decide for themselves whether a notification to the MLRO should be made.

6. An Employee, including the MLRO, who considers that a Person has engaged in or is engaging in activity or Transactions that he knows or suspects to be suspicious would not be expected to know the exact nature of the criminal offence or that the particular funds were definitely those arising from the crime of money laundering or terrorist financing.

7. Activity or Transactions that appear unusual are not necessarily suspicious. Even customers with a stable and predictable Transaction profile will have periodic Transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of Transactions or account activity. So the unusual is, in the first instance, only a basis for further inquiry, which may in turn require judgement as to whether it is suspicious. A Transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report it then arises.

8. Effective CDD measures may provide the basis for recognising unusual and suspicious activity and Transactions. Refusal to provide documentation to support CDD or refusal to disclose a beneficial owner may be considered suspicious activity. Where there is a customer relationship, suspicious activity will often be one that is inconsistent with a customer's known legitimate activity, or with the normal business activities for that type of account or customer. Therefore, the key to recognising "suspicious activity" is knowing enough about the customer and the customer's normal expected activities to recognise when their activity is abnormal.

9. A Relevant Person may consider implementing policies and procedures whereby disciplinary action is taken against an Employee who fails to notify the Relevant Person's MLRO.

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

### 14.3 Suspicious Activity/Transaction Reports

14.3.1 A Relevant Person must ensure that where the Relevant Person's MLRO receives an internal notification of suspicious activity under Rule 14.2.2, the MLRO, without delay:

(a) investigates and documents the circumstances in relation to which the notification made under Rule 14.2.2 was made;

(b) determines whether in accordance with Federal AML Legislation a SAR/STR must be made and documents such determination; and

(c) if required, make a SAR/STR as soon as practicable.

14.3.2 The MLRO must, following receipt of an internal notification of suspicious activity under Rule 14.2.2, document:

(a) the steps taken to investigate the circumstances in relation to which the internal notification is made; and

(b) where no external SAR/STR is made, the reasons why no such report was made.

14.3.3 Where, following a notification to the MLRO of suspicious activity under 14.2.2, no SAR/STR is made, a Relevant Person must record the reasons for not making a SAR/STR.

14.3.4 A Relevant Person must ensure that if the MLRO decides to make a SAR/STR, 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. 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.

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.

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.

## 14.4 Suspension of Transactions and "no tipping-off" requirement

14.4.1 A Relevant Person must not carry out Transactions that it knows or suspects or has reasonable grounds for knowing or suspecting to be related to money laundering or terrorist financing until it has informed the FIU pursuant to Rule 14.3.1.

**Guidance**

1. Relevant Persons are reminded that in accordance with Federal AML Legislation, Relevant Persons or any of their Employees must not tip off any Person, that is, inform any Person that he is being scrutinised, or investigated by any other competent authority, for possible involvement in suspicious Transactions or activity related to money laundering or terrorist financing.

2. If a Relevant Person reasonably believes that performing CDD measures will tip off a customer or potential customer, it may choose not to pursue that process and should file a Suspicious Activity/Transaction Report. Relevant Persons should ensure that their Employees are aware of and sensitive to these issues when considering the CDD measures.

### 14.5 Record-keeping

14.5.1 All relevant details of any notification to the MLRO under Rule 14.2 or Suspicious Activity/Transaction Reports filed pursuant to Rule 14.3 must be kept for at least six years from the date on which the report was made.

### 14.6 Freezing of assets

**Guidance**

The Regulator has certain powers under FSMR to impose a requirement restricting an Authorised Person or Recognised Body from disposing of or transferring property including, for example, assets or other funds suspected of relating to money laundering. It may also apply to the ADGM Courts for an order restraining a Person from transferring or disposing of any assets suspected of relating to money laundering or terrorist financing. In cases involving suspected money laundering or terrorist financing, the Regulator will usually take such action in coordination with the FIU.

## 15. DNFBP REGISTRATION AND SUPERVISION

### 15.1 Criteria for registration as a DNFBP

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 whether an applicant is fit and proper under (1)(a), the Regulator may, without limiting the matters it may take into account, consider the applicant, its 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 applicant is fit and proper, consider the cumulative effect of factors which, if taken individually, may be regarded as insufficient to give reasonable cause to doubt the fitness and propriety of an applicant.

### 15.2 Application for registration as a DNFBP

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.

15.2.2 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.

15.2.3 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 DNFBP notifications

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) Governing Body;

(f) Senior Management; or

(g) Beneficial Ownership.

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.

## 15.4 Disclosure of regulatory status

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.

## 15.5 Co-ordination between the Regulator and the Registrar of Companies

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 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. NON-PROFIT ORGANISATIONS

### 16.1 Responsibility for NPO compliance

**16.1.1** An NPO's Governing Body is responsible for establishing, maintaining and monitoring the NPO's obligations under this chapter.

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;

(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.

### 16.2 Record Keeping

16.2.1 An NPO must maintain for a period of at least six years records of its obligations required under Rule 16.1.2, covering both domestic and international transactions, which are sufficiently detailed to verify that funds have been received and spent in a manner consistent with the purpose and objectives of the NPO.

### 16.3 Co-operation

16.3.1 An NPO must deal with the Regulator in an open and co-operative manner and keep the Regulator informed of significant events or anything else relating to the NPO of which the Regulator would reasonably expect to be notified.

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;

(b) make its Employees readily available for meetings with the Regulator;

(c) give the Regulator access to any information, Documents, records, files, tapes, computer data or systems, which are within the NPO's possession or control and provide any facilities to the Regulator;

(d) permit the Regulator to copy Documents or other material on the premises of the NPO at the NPO's expense;

(e) provide any copies of those Documents or other material as requested by the Regulator; and

(f) answer truthfully, fully and promptly, all questions which are put to it by 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 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.