



The DFSA Rulebook

Ancillary Service Providers Module

(ASP)

Contents

The contents of this module are divided into the following chapters, sections and appendices:

| | | |
|----------|--|-----------|
| 1 | APPLICATION | 3 |
| 1.1 | Application..... | 3 |
| 2 | DEFINITION OF ANCILLARY SERVICES | 4 |
| 2.1 | Definition | 4 |
| 2.2 | By way of business..... | 4 |
| 2.3 | Definitions..... | 5 |
| 3 | GENERAL PROVISIONS | 7 |
| 3.1 | Application..... | 7 |
| 3.2 | Interpretation | 7 |
| 3.3 | Disclosure of regulatory status | 8 |
| 3.4 | [Deleted] [VER6/12-07] [RM52/07]..... | 8 |
| 3.5 | Communication with the DFSA | 8 |
| 4 | REGULATORY PROCESSES..... | 9 |
| 4.1 | Application..... | 9 |
| 4.2 | Applications to carry on ancillary services..... | 9 |
| 4.3 | Notifications..... | 10 |
| 4.4 | Information gathering and access to premises..... | 10 |
| 4.5 | Variation or withdrawal of registration | 11 |
| 4.6 | Variation or withdrawal on the DFSA's initiative | 11 |
| 4.7 | Other powers of enforcement..... | 12 |
| 5 | ANTI MONEY LAUNDERING OFFICER..... | 13 |
| 5.1 | Application..... | 13 |
| 5.2 | Requirements..... | 13 |

6 ANTI MONEY LAUNDERING RULES APPLYING TO ANCILLARY SERVICES¹⁴

| | | |
|------|--|----|
| 6.1 | Application..... | 14 |
| 6.2 | General requirements..... | 14 |
| 6.3 | Co-operation with regulators | 15 |
| 6.4 | Appointment, responsibilities and duties of the AMLO | 16 |
| 6.5 | Customer identification requirements..... | 18 |
| 6.6 | Internal and external reporting requirements | 23 |
| 6.7 | Tipping-off | 25 |
| 6.8 | Government, regulatory and international findings..... | 26 |
| 6.9 | Money laundering risks | 27 |
| 6.10 | Awareness and training..... | 28 |

APP1 [DELETED] [VER6/12-07] [RM52/07] 30**APP2 CUSTOMER IDENTIFICATION REQUIREMENTS 31**

| | | |
|------|----------------------------------|----|
| A2.1 | Duties and responsibilities..... | 31 |
|------|----------------------------------|----|

APP3 MONEY LAUNDERING RISKS 38

| | | |
|------|--|----|
| A3.1 | Risk assessment | 38 |
| A3.2 | Risks regarding corruption and politically exposed persons | 39 |
| A3.3 | Suspicious transactions and transaction monitoring | 40 |



1 APPLICATION

1.1 Application

- 1.1.1** This module (ASP) applies to every Person to whom the Regulatory Law 2004 applies and to the same extent in relation to every such Person of the Regulatory Law 2004, except to the extent that a provision of ASP provides for a narrower application.

2 DEFINITION OF ANCILLARY SERVICES

2.1 Definition

Guidance

Article 44(1) of the Regulatory Law 2004 prohibits a Person from carrying on an Ancillary Service in or from the DIFC unless the Person is registered as an Ancillary Service Provider. The activities which constitute Ancillary Services are prescribed in this chapter.

- 2.1.1** (1) An activity constitutes an Ancillary Service under the Regulatory Law 2004 and these Rules where:
- (a) it is an activity specified in (2); and
 - (b) such activity is carried on by way of business in the manner described in section 2.2.
- (2) The activities for the purposes of (1) are:
- (a) Providing Legal Services;
 - (b) Providing Accountancy Services;
- (3) Each kind of activity specified in (2):
- (a) is to be construed in the manner provided under these Rules; and
 - (b) is subject to exclusions under these Rules which may apply to such an activity.

2.2 By way of business

- 2.2.1** A Person carries on an activity specified in Rule 2.1.1(2) by way of business only if he carries on that activity from a permanent place of business maintained by him in the DIFC and engages in that activity in a manner which constitutes the carrying on of a business by him.

Exclusions

- 2.2.2** An individual does not carry on an activity specified in Rule 2.1.1(2) by way of business if he carries on that activity solely as an employee who is employed or appointed under a contract of service.
- 2.2.3** A Person does not carry on an activity specified in Rule 2.1.1(2) by way of business if that Person is a Body Corporate and carries on the activity solely as principal with or for other Bodies Corporate:
- (a) which are within the same Group; or
 - (b) which are or propose to become participants in a joint enterprise and the transaction is entered into for the purposes of or in connection with that enterprise.
- 2.2.4** A person does not carry on an activity specified in Rule 2.1.1(2) by way of business if such a Person is an agency or other body created by or under Dubai Law to the extent that it exercises a power or performs a function relating to the governance or regulation of the DIFC.

2.3 Definitions**Providing legal services**

- 2.3.1** In Rule 2.1.1, Providing Legal Services means the application of legal principles or judgement with regard to the circumstances of another Person who is an Authorised Firm or Authorised Market Institution, including but not limited to:
- (a) giving legal advice or counsel to such a Person as to his legal rights or the legal rights or responsibilities of others;
 - (b) giving legal advice or counsel to such a Person in relation to any DIFC law or legislation made thereunder;
 - (c) drafting or completion of legal documents or agreements which affect such a Person's legal rights;
 - (d) representation of such a Person in court proceedings or in an administrative adjudicative procedure in which legal pleadings are filed or a record is established as the basis for judicial review; or

- (e) negotiation of legal rights or responsibilities on behalf of such a Person; but excluding acting as a lay representative authorised by an administrative agency or tribunal, serving as a judge, mediator, arbitrator, conciliator or facilitator; and participation in employment negotiations, arbitrations or conciliations.

Providing accountancy services]

2.3.2 In Rule 2.1.1, Providing Accountancy Services means the application of accounting principles or judgement with regard to the circumstances of another Person who is an Authorised Firm or Authorised Market Institution, including but not limited to the following:

- (a) performing audit, examination, verification, investigation, certification, presentation or review of financial transactions and accounting records for such a Person;
- (b) preparing or certifying reports on audits or examinations of books or records of account, balance sheets, and other financial, accounting and related documents for such a Person; or
- (c) advising such a Person on matters relating to accounting procedure and the recording, presentation or certification of financial information or data, including financial information or data required by legislation applicable in the DIFC.

3 GENERAL PROVISIONS

3.1 Application

3.1.1 Section 3.2 applies to every Person to whom any provision of the ASP module applies.

3.1.2 Section 3.3 applies to every Ancillary Service Provider.

3.1.3 Section 3.4 applies to every Ancillary Service Provider and applicant for registration as an Ancillary Service Provider.

3.2 Interpretation

Guidance

1. Every provision in the ASP module should be interpreted in the light of its purpose. The purpose of any provision is to be gathered first and foremost from the text of the provision in question and its context among other relevant provisions.
2. Where this section refers to a provision, this means every type of provision, including Rules and Guidance.
3. Where reference is made in ASP to another provision of the Rulebook or to another provision of DIFC legislation, it is a reference to that provision as amended from time to time.
4. Unless the contrary intention appears:
 - a. words in the Rulebook importing the masculine gender include the feminine gender and words importing the feminine gender include the masculine; and
 - b. words in the Rulebook in the singular include the plural and words in the plural include the singular.
5. If a provision in the Rulebook refers to a communication, notice, agreement, or other documents 'in writing' then, unless the contrary intention appears, it means in legible form and capable of being reproduced on paper, irrespective of the medium used. Expressions related to writing must be interpreted accordingly.
6. Any reference to 'dollars' ('\$') is a reference to United States Dollars unless the contrary intention appears.

7. References to Articles made throughout the Rulebook are references to the Regulatory Law 2004 unless otherwise stated.
8. Unless stated otherwise, a day means a calendar day. If an obligation falls on a calendar day which is either a Friday or Saturday or an official State holiday in the DIFC, the obligation must take place on the next calendar day which is a business day. [Amended][VER4/02-07][RM42/07]

Defined terms

9. Defined terms are identified throughout the Rulebook by the capitalisation of the initial letter of a word or phrase and are defined in the Glossary (GLO). Unless the context otherwise requires, where capitalisation of the initial letter is not used, an expression has its natural meaning.

3.3 Disclosure of regulatory status

- 3.3.1** An Ancillary Service Provider must not misrepresent its status expressly or by implication.
- 3.3.2** The DFSA logo must not be reproduced by an Ancillary Service Provider without express written permission from the DFSA and in accordance with any conditions for use.

3.4 [Deleted] [VER6/12-07] [RM52/07]

3.5 Communication with the DFSA

- 3.5.1** An Ancillary Service Provider must ensure that any communication with the DFSA is conducted in the English language.

4 REGULATORY PROCESSES

4.1 Application

4.1.1 This chapter applies to every Ancillary Service Provider and applicant for registration as an Ancillary Service Provider.

Guidance

The purpose of this chapter is to set out requirements and to give Guidance in relation to the processes for registration, supervision and enforcement.

4.2 Applications to carry on ancillary services

4.2.1 A Person seeking registration as an Ancillary Service Provider must apply to the DFSA for authority to carry on one or more specified Ancillary Services.

4.2.2 Applications for registration may be submitted only by a Body Corporate or Partnership.

4.2.3 An applicant must complete and submit the appropriate forms in AFN.

4.2.4 An Authorised Market Institution will not be registered as an Ancillary Service Provider.

Guidance

An Authorised Firm may be an Ancillary Service Provider, and an Ancillary Service Provider may also be licensed as an Authorised Firm.

4.2.5 When the DFSA is considering an application for registration the DFSA will consider any matter which may harm or may have harmed the integrity or the reputation of the DFSA or DIFC.

Guidance

1. The DFSA will have particular regard to whether the firm, or anyone in a position of influence in or over it, has criminal convictions or been the subject of adverse findings by courts or regulatory authorities in the UAE or elsewhere, or is known to have engaged in dishonest or improper business practices.
2. A Person who provides information to the DFSA which is false, misleading or deceptive, or who conceals information where the concealment is likely to mislead or deceive the DFSA, commits a contravention of Article 66.

- 4.2.6** An applicant may appeal to the Regulatory Appeals Committee against a refusal to grant an application for registration, and the Regulatory Appeals Committee has jurisdiction to hear such an appeal.

Guidance

Under Article 60(3) of the Regulatory Law 2004, the DFSA may in its absolute discretion grant or refuse to grant an application for registration.

4.3 Notifications

- 4.3.1** This section does not apply to an Ancillary Service Provider which is also an Authorised Firm.

- 4.3.2** An Ancillary Service Provider must notify the DFSA as soon as practical of any change in its:

- (a) name;
- (b) legal status; or
- (c) address.

4.4 Information gathering and access to premises

Guidance

1. Article 73 provides the DFSA with powers to require Ancillary Service Providers and their officers, employees and agents by written notice to:
 - a. give, or procure the giving of, such specified information; or
 - b. produce, or procure the production of, such specified documents;to the DFSA as the DFSA considers necessary or desirable to meet the objectives of the DFSA.
2. Under Article 73, the DFSA may also enter the premises of any Ancillary Service Provider during normal business hours or at any other time as may be agreed for the purpose of inspecting and copying information or documents stored in any form on such premises, as it considers necessary or desirable to meet the objectives of the DFSA.
3. Where the DFSA gives notice under Article 73, it will expect full co-operation from the Ancillary Service Provider.

4.5 Variation or withdrawal of registration

Guidance

Under Article 60(4), the DFSA may make Rules setting out how and on what grounds registration may be varied or withdrawn.

- 4.5.1** (1) The DFSA may:
- (a) withdraw an Ancillary Service Provider's registration; or
 - (b) change an Ancillary Service Provider's scope of authority under a registration;
- either on its own initiative or at the request of the Ancillary Service Provider.
- (2) In (1) if the Ancillary Service Provider requests the change it must apply using the appropriate form in AFN.
- 4.5.2** Upon deciding to exercise its powers under Rule 4.5.1 the DFSA shall without delay inform the Ancillary Service Provider in writing of:
- (a) such decision;
 - (b) the Ancillary Services to which it relates; and
 - (c) the date on which the decision shall be deemed to take effect.

4.6 Variation or withdrawal on the DFSA's initiative

- 4.6.1** The DFSA may exercise the power set out in Rule 4.5.1 on its own initiative only if it is satisfied that:
- (a) the Ancillary Service Provider has failed to carry on an Ancillary Service in the DIFC for a continuous period of 12 months or more; or
 - (b) the Ancillary Service Provider has breached, or is breaching, the Regulatory Law 2004, Rules or other legislation administered by the DFSA.
- 4.6.2** The DFSA may exercise the power set out in Rule 4.5.1 to vary or withdraw registration on its own initiative only if it has given the relevant Ancillary Service Provider a suitable opportunity to make representations in person and in writing to the DFSA in relation to the proposed action.

4.6.3 Rule 4.6.2 does not apply if the DFSA concludes that any delay likely to arise as a result of such requirement is prejudicial to the interests of the DIFC.

Guidance

1. Generally, the DFSA will only consider exercising the power set out in Rule 4.5.1 on its own initiative after a thorough investigation.
2. If, having considered the results of the investigation, the Enforcement Decisions Committee considers that it may be necessary to exercise this power, it will refer the matter to a nominated DFSA officer, referred to as the Decision Maker. The Decision Maker shall consider the matter impartially.
3. The Decision Maker will follow by analogy the procedure set out in ENF App2.

4.6.4 An Ancillary Service Provider may appeal to the Regulatory Appeals Committee against a decision to vary or withdraw its registration, and the Regulatory Appeals Committee has jurisdiction to hear such an appeal.

4.7 Other powers of enforcement

Guidance

Although the Rules and Guidance specific to Ancillary Service Providers appear in this module, the DFSA has some powers of enforcement and intervention which apply to Ancillary Service Providers as they apply to other firms and individuals. These powers are dealt with in ENF, and some Rules and Guidance in that module therefore apply to Ancillary Service Providers.

5 ANTI MONEY LAUNDERING OFFICER

5.1 Application

5.1.1 This chapter applies to every Ancillary Service Provider and applicant for registration as an Ancillary Service Provider except where the Ancillary Service Provider or applicant is an Authorised Firm.

5.2 Requirements

5.2.1 (1) An Ancillary Service Provider or applicant must designate an Anti Money Laundering Officer (AMLO), who will be directly responsible for the Ancillary Service Provider's compliance with applicable anti money laundering legislation.

(2) It must do so by completing and filing with the DFSA the appropriate form in AFN.

5.2.2 The AMLO must be ordinarily resident in the U.A.E.

5.2.3 If the AMLO leaves the employment of the relevant Ancillary Service Provider, the Ancillary Service Provider must designate a successor within 28 days.

6 ANTI MONEY LAUNDERING RULES APPLYING TO ANCILLARY SERVICES

6.1 Application

- 6.1.1** (1) This chapter applies to every Ancillary Service Provider.
- (2) Some provisions also relate to the AMLO of an Ancillary Service Provider in his capacity as an individual designated in accordance with chapter 5.

Guidance

1. The Rules in this Chapter require Ancillary Service Providers to have adequate policies, procedures, systems and controls in place to prevent the activity of money laundering. Money laundering is generally described as the process by which criminals attempt to hide or disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of criminal funds. This includes the closely related subject of ‘terrorist financing’ and international efforts to locate and cut off the funding of terrorists and their organisations.
2. Accordingly, where the DFSA uses the term ‘money laundering’, Ancillary Service Providers are required to include ‘terrorist financing’ in all considerations with regard to their policies, procedures, systems and controls such as those relating to suspicious transaction reporting. [Amended][VER5/06/07][RM43/07]

6.2 General requirements

- 6.2.1** (1) An Ancillary Service Provider must establish and maintain effective anti money laundering policies, procedures, systems and controls to prevent opportunities for Money Laundering in relation to the Ancillary Service Provider and its activities.
- (2) An Ancillary Service Provider must take reasonable steps to ensure that its Employees comply with the relevant requirements of its anti money laundering policies, procedures, systems and controls.

Guidance

1. An Ancillary Service Provider’s anti money laundering policies, procedures, systems and controls should:
 - a. ensure compliance with the U.A.E. Law No.4 and any other relevant Federal laws;
 - b. enable suspicious customers and transactions to be detected and reported;

- c. ensure the Ancillary Service Provider is able to provide an audit trail of a transaction; and
 - d. comply with any other obligation in these Rules.
2. An Ancillary Service Provider's anti money laundering compliance arrangements should consist of policies, procedures, systems and controls and may also encompass appropriate anti money laundering programmes and strategies.
3. An Ancillary Service Provider should have a policy statement detailing the duties and obligations of its AMLO.
4. An Ancillary Service Provider should have specific arrangements to consider the fitness and propriety of its staff. The arrangements should take into account criminal convictions, adverse findings by courts or regulatory authorities in the U.A.E. or elsewhere, or engagement in dishonest or improper business practices.
5. Under Article 3 of the U.A.E. Law No.4, an Ancillary Service Provider may be criminally liable for the offence of Money Laundering if such an activity is intentionally committed in its names or for its accounts.

6.2.2 Ancillary Service Provider which is a Domestic Firm must ensure that its anti money laundering policies, procedures, systems and controls apply to any branch or subsidiary operating in another jurisdiction.

6.2.3 If another jurisdiction's laws or regulations prevent or inhibit an Ancillary Service Provider from complying with the U.A.E. Law No.4 or with these Rules, the Ancillary Service Provider must promptly inform the DFSA in writing.

Guidance

1. If the DFSA is not satisfied in respect of anti money laundering compliance in the circumstances set out in Rule 6.2.3 it may notify the Ancillary Service Provider that the DFSA will withdraw the Ancillary Service Provider's registration if it operates a branch or subsidiary in the relevant jurisdiction.
2. A Domestic Firm should conduct a periodic review to verify that any branch or subsidiary operating in another jurisdiction is in compliance with the obligations imposed under the U.A.E. Law No. 4 of 2002 regarding Criminalisation of Money Laundering and these Rules.

6.3 Co-operation with regulators

6.3.1 An Ancillary Service Provider that receives a request for information from a regulator or agency responsible for anti money laundering regarding enquiries into potential money laundering related to Ancillary Services carried on in or from the DIFC, must promptly inform the DFSA in writing.

6.4 Appointment, responsibilities and duties of the AMLO

Appointment

Guidance

1. The requirement to designate an individual as the AMLO is in Rule 5.2.1.
2. Pursuant to Rule 5.2.2 the AMLO must be ordinarily resident in the U.A.E.

6.4.1 An Ancillary Service Provider must ensure that the AMLO is of sufficient seniority within the Ancillary Service Provider to enable him to:

- (a) act on his own authority;
- (b) have direct access to the governing body and senior management;
- (c) have sufficient resources including, if necessary, an appropriate number of appropriately trained Employees to assist in the performance of his duties in an effective, objective and independent manner;
- (d) have unrestricted access to information the Ancillary Service Provider has about the financial and business circumstances of a customer or any Person on whose behalf the customer is or has been acting; and
- (e) have unrestricted access to relevant information about the features of the transaction which the Ancillary Service Provider has entered into or may have contemplated entering into with or for the customer or that Person.

Responsibilities

- #### **6.4.2**
- (1) An Ancillary Service Provider must ensure that its AMLO is responsible for all of its anti money laundering activities carried on in or from the DIFC.
 - (2) An Ancillary Service Provider must ensure that its AMLO carries out and is responsible for the following:
 - (a) establishing and maintaining the Ancillary Service Provider's anti money laundering policies, procedures, systems and controls and compliance with anti money laundering legislation applicable in the DIFC;
 - (b) the day-to-day operations for compliance with the Ancillary Service Provider's anti money laundering policies, procedures, systems and controls;

- (c) acting as the point of contact to receive internal Suspicious Transaction Reports from the Ancillary Service Provider's Employees pursuant to Rule 6.6.1;
- (d) taking appropriate action pursuant to Rule 6.6.2 following the receipt of an internal Suspicious Transaction Report from the Ancillary Service Provider's staff;
- (e) making, in accordance with U.A.E. Law No. 4 of 2002 regarding Criminalisation of Money Laundering, external Suspicious Transaction Reports to the Anti Money Laundering Suspicious Cases Unit (AMLSCU) of the U.A.E. (if appropriate) and sending corresponding copies to the DFSA under Rule 6.6.2;
- (f) acting as the point of contact within the Ancillary Service Provider for competent U.A.E. authorities and the DFSA regarding money laundering issues;
- (g) responding promptly to any request for information made by competent U.A.E. authorities or the DFSA; and
- (h) establishing and maintaining an appropriate anti money laundering training programme and adequate awareness arrangements pursuant to Rules under section 6.10.

Guidance

Where an Ancillary Service Provider outsources specific anti money laundering tasks of its AMLO to another individual or a third party provider, including within a corporate Group, the AMLO of the Ancillary Service Provider remains responsible for ensuring compliance with the duties imposed on the AMLO. The Ancillary Service Provider should satisfy itself of the suitability of anyone who acts for it.

Reporting

6.4.3 The AMLO must report at least annually to the governing body or senior management of the Ancillary Service Provider on the following matters:

- (a) the Ancillary Service Provider's compliance with applicable anti money laundering laws including Rules;
- (b) the quality of the Ancillary Service Provider's anti money laundering policies, procedures, systems and controls;
- (c) any internal Suspicious Transaction Reports made by the Ancillary Service Provider's staff pursuant to Rule 6.6.1 and action taken in respect of those reports, including the grounds for all decisions;

- (d) any external Suspicious Transaction Reports made by the Ancillary Service Provider pursuant to Rule 6.6.2 and action taken in respect of those reports including the grounds for all decisions; and
 - (e) any other relevant matters related to money laundering as it concerns the Ancillary Service Provider's business.
- 6.4.4** An Ancillary Service Provider must ensure that its governing body or senior management promptly:
- (a) assess the report provided under Rule 6.4.3;
 - (b) take action, as required subsequent to the findings of the report, in order to resolve any identified deficiencies; and
 - (c) make a record of their assessment in (a) and the action taken in (b).
- 6.4.5** (1) The report provided under Rule 6.4.4 and the records of the assessment and actions pursuant to Rule 6.4.4(c) must be documented in writing.
- (2) A complete copy of each must be provided to the DFSA within two months of the Ancillary Service Provider's financial year end.

6.5 Customer identification requirements

Duties and responsibilities

- 6.5.1** (1) Subject to the exception under Rule 6.5.5, an Ancillary Service Provider must establish and verify the identity of any customer with or for whom the Ancillary Service Provider acts or proposes to act.
- (2) In establishing and verifying a customer's true identity, an Ancillary Service Provider must obtain sufficient and satisfactory evidence having considered:
- (a) its risk assessment under Rule 6.9.1 in respect of the customer; and
 - (b) the relevant provisions of App2 and App3.
- (3) An Ancillary Service Provider must update as appropriate any customer identification policies, procedures, systems and controls.

Guidance

An Ancillary Service Provider should adopt a risk-based approach for the customer identification and verification process. Depending on the outcome of the Ancillary Service Provider's money laundering risk assessment of its customer, it should decide to what level of detail the customer identification and verification process will need to be performed.

- 6.5.2** (1) Subject to the exception under Rule 6.5.5, whenever an Ancillary Service Provider comes into contact with a customer with or for whom it acts or proposes to act, it must establish whether the customer is acting on his own behalf or on the behalf of another Person.
- (2) An Ancillary Service Provider must establish and verify the identity of both the customer and any other Person on whose behalf the customer is acting, including that of the Beneficial Owner of the relevant funds, which may be the subject of a transaction to be considered, and must obtain sufficient and satisfactory evidence of their identities.

Guidance

An Ancillary Service Provider should obtain a statement from a prospective customer to the effect that he is, or is not, acting on his own behalf. In cases where the customer is acting on behalf of third parties, it is recommended that the Ancillary Service Provider obtains a written statement, confirming the statement made by the customer, from the parties including that of the Beneficial Owner.

- 6.5.3** (1) The obligations under Rules 6.5.1 and 6.5.2 must be fulfilled before the Ancillary Service Provider effects any transaction on behalf of the customer.
- (2) It is an Ancillary Service Provider's responsibility when it next has contact with a customer who was an existing customer, prior to the Ancillary Service Provider's registration by the DFSA, to assess whether it has performed the identification of that customer which would have been required had these Rules been applicable when the customer became a customer, and to obtain without delay any missing information or evidence about the true identity of all relevant parties.
- 6.5.4** (1) An Ancillary Service Provider must ensure that the information and documentation concerning a customer's identity remains accurate and up-to-date.
- (2) If at any time an Ancillary Service Provider becomes aware that it lacks sufficient information or documentation concerning a customer's identification, or develops a concern about the accuracy of its current information or documentation, it must promptly obtain appropriate material to verify the customer's identity.

Guidance

An Ancillary Service Provider should undertake a periodic review to ensure that customer identity documentation is accurate and up-to-date.

Exception to customer identification requirements

- 6.5.5** (1) Subject to Rule 6.5.7, an Ancillary Service Provider is not required to establish the identity of a customer pursuant to Rule 6.5.1 if the customer is one of the following:
- (a) an Authorised Firm;
 - (b) an Ancillary Service Provider;
 - (c) an Authorised Market Institution;
 - (d) a credit institution or other financial institution covered by equivalent identification requirements as set out in (2); or
 - (e) a Person who is subject to anti money laundering legislation equivalent to the provisions in this chapter or subject to equivalent international standards applying in FATF countries.
- (2) An institution falls within (1)(d) if it is:
- (a) a credit institution or other financial institution whose entire operations are subject to regulation, including anti money laundering, by:
 - (i) a Financial Services Regulator in an FATF Country; or
 - (ii) another relevant authority in a FATF Country; or
 - (b) a subsidiary of a credit institution or other financial institution referred to in (2)(a), provided that the law that applies to the parent company ensures that the subsidiary also observes the same provisions.

Guidance

1. The DFSA would expect an Ancillary Service Provider to take reasonable steps to determine whether or not a customer falls within the exceptions under this Rule, and to keep records of the basis on which a customer was considered to be exempt.
2. For the purposes of Rule 6.5.5(1)(d) and 6.5.5(2) proof of a prospective customer by a Financial Services Regulator or another relevant authority should be obtained. For the purpose of Rule 6.5.5(1)(e) this proof should be obtained by a regulator or another relevant authority. In cases of doubt, the DFSA expects an Ancillary Service Provider to perform the complete identification of a prospective customer as specified in Rule 6.5.1.

3. For the purposes of Rule 6.5.5(2)(b), an Ancillary Service Provider should obtain a written statement from both the parent company and the subsidiary in question, stamped with the company's seal and signed by authorised signatories, confirming that the subsidiary falls under the same anti money laundering provisions as the parent company.

6.5.6 Subject to Rule 6.5.7, an Ancillary Service Provider is not required to establish the beneficial ownership pursuant to Rule 6.5.2 if the Ancillary Service Provider's customer is a Person falling within Rule 6.5.5.

6.5.7 (1) Rules 6.5.5 and 6.5.6 do not apply where the Ancillary Service Provider:

- (a) knows or suspects; or
- (b) has reasonable grounds to know or suspect;

that a customer or a Person on whose behalf he is acting is engaged in Money Laundering.

- (2) The Ancillary Service Provider will be taken to know or suspect or to have reasonable grounds to know or suspect, if:

- (a) any Employee handling the transaction or potential transaction; or
- (b) anyone managerially responsible for it;

knows or suspects or has reasonable grounds to know or suspect that a customer or a Person on whose behalf he is acting is engaged in Money Laundering.

Documentation and records

6.5.8 (1) All relevant information, correspondence and documentation used by an Ancillary Service Provider to verify a customer's identity pursuant to Rules 6.5.1 and 6.5.2 must be kept for at least six years from the date on which the business relationship with a customer has ended.

- (2) If the date on which the business relationship with a customer has ended remains unclear, it may be taken to have ended on the date of the completion of the last transaction.

Guidance

1. The records maintained by an Ancillary Service Provider should be kept in such a manner that:
 - a. the DFSA or another competent third party is able to assess the Ancillary Service Provider's compliance with legislation applicable in the DIFC;

- b. any transaction which was processed by or through the Ancillary Service Provider on behalf of a customer or other third party can be reconstructed;
- c. any customer or third party can be identified;
- d. all internal and external Suspicious Transaction Reports can be identified; and
- e. the Ancillary Service Provider can satisfy, within an appropriate time, any regulatory enquiry or court order to disclose information.

6.5.9 All relevant details of any transaction carried out by the Ancillary Service Provider with or for a customer must be kept for at least six years from the date on which the transaction was completed.

Reliance on others to verify identity

6.5.10 An Ancillary Service Provider may delegate technical aspects of the customer identification process to a qualified professional.

Guidance

- 1. The delegation of aspects of the identification process to qualified professionals does not release the Ancillary Service Provider from any of its obligations under applicable laws including Rules.
- 2. If the identification process has not been performed in accordance with these Rules, the Ancillary Service Provider is expected to perform the identification process itself.

6.5.11 (1) Where a customer is introduced by another member of the Ancillary Service Provider's Group, an Ancillary Service Provider need not re-identify the customer, provided that:

- (a) the identity of the customer has been verified by the other member of the Ancillary Service Provider's Group in a manner consistent with this chapter or equivalent international standards applying in FATF Countries;
- (b) no exception from identification obligations has been applied in the original identification process; and
- (c) a written statement is received from the introducing member of the Ancillary Service Provider's Group confirming that:
 - (i) the customer has been identified with the relevant standards under (a) and (b);
 - (ii) any identification evidence can be accessed by the Ancillary Service Provider without delay; and
 - (iii) that the identification evidence is kept for at least a six years.

- (2) If an Ancillary Service Provider is not satisfied that the customer has been identified in a manner consistent with these Rules, the Ancillary Service Provider must perform the verification process itself.

6.5.12 (1) Where customer identification records are kept by the Ancillary Service Provider or other Persons outside the U.A.E., an Ancillary Service Provider must take reasonable steps to ensure that the records are held in a manner consistent with these Rules.

- (2) An Ancillary Service Provider must verify if there is secrecy or data protection legislation that would restrict access to such data by the Ancillary Service Provider, the DFSA or the law enforcement agencies of the U.A.E. Where such legislation exists, the Ancillary Service Provider must obtain without delay certified copies of the relevant identification evidence and keep these copies in a jurisdiction which allows access by all those Persons.

6.5.13 An Ancillary Service Provider must not:

- (a) establish a relationship with a Shell Bank;
- (b) establish or keep anonymous accounts or accounts in false names; or
- (c) maintain a nominee account which is held in the name of one Person, but controlled by or held for the benefit of another Person whose identity has not been disclosed to the Ancillary Service Provider.

6.6 Internal and external reporting requirements

6.6.1 (1) An Ancillary Service Provider must have appropriate arrangements to ensure that whenever any Employee, acting in the ordinary course of his employment, either:

- (a) knows or suspects; or
- (b) has reasonable grounds for knowing or suspecting;

that a Person is engaged in Money Laundering, that Employee makes an internal Suspicious Transaction Report to the Ancillary Service Provider's AMLO.

- (2) An Ancillary Service Provider must have policies and procedures to ensure that disciplinary action can be taken against any Employee who fails to make such a report.

Guidance

The requirement for Employees to make an internal Suspicious Transaction Report should include situations when no business relationship was developed because the circumstances were suspicious.

6.6.2 If an Ancillary Service Provider's AMLO receives an internal Suspicious Transaction Report he must without delay:

- (a) investigate the circumstances in relation to which the report was made;
- (b) determine whether in accordance with U.A.E. Law No. 4 of 2002 regarding Criminalisation of Money Laundering, a corresponding external Suspicious Transaction Report must be made to the AMLSCU (if appropriate);
- (c) if required, make such an external report to the AMLSCU; and
- (d) provide a copy of such an external report to the DFSA at the time of provision under U.A.E. Law No. 4 of 2002 regarding Criminalisation of Money Laundering.

Guidance

- 1. An Ancillary Service Provider may allow its Employees to consult with their line managers before sending a report to the AMLO. The DFSA would expect that such consultation does not prevent making a report whenever an Employee has stated that he has knowledge, suspicion or reasonable grounds for knowing or suspecting that a transaction may involve money laundering.
- 2. Ancillary Service Providers are reminded that the failure to report suspicions of Money Laundering may constitute a criminal offence that is punishable under the laws of the U.A.E.
- 3. External Suspicious Transaction Reports under U.A.E. Law No. 4 of 2002 regarding Criminalisation of Money Laundering should be faxed to the AMLSCU and a copy faxed to the DFSA. The dedicated fax numbers and the template for making Suspicious Transaction Reports are available on the DFSA website.

6.6.3 The AMLO must document:

- (a) the steps taken to investigate the circumstances in relation to which an internal Suspicious Transaction Report is made; and
- (b) where no external Suspicious Transaction Report is made to the AMLSCU, the reasons why no such report was made.

6.6.4 All relevant details of any internal and external Suspicious Transaction Report pursuant to Rules 6.6.1 and 6.6.2 must be kept for at least six years from the date on which the report was made.

- 6.6.5** An Ancillary Service Provider must ensure that if the AMLO decides to make an external Suspicious Transaction Report in accordance with Rule 6.6.2, his decision is made independently and is not subject to the consent or approval of any other Person.
- 6.6.6** Ancillary Service Providers must not carry out transactions which they know or suspect or have reasonable grounds for knowing or suspecting to be related to Money Laundering until they have informed the AMLSCU (if appropriate) and the DFSA pursuant to Rule 6.6.2.

Guidance

1. In preparation of an external Suspicious Transaction Report, if an Ancillary Service Provider 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 Ancillary Service Provider's proposed course of further action in relation to the case should be included in the report.
2. If the Ancillary Service Provider has reported a suspicion to the AMLSCU, it may instruct the Ancillary Service Provider on how to proceed with the transaction. If the customer in question expresses his wish to move the funds before an Ancillary Service Provider receives instruction from the AMLSCU (if appropriate) on how to proceed, the Ancillary Service Provider should immediately contact the AMLSCU for further instructions.

6.7 Tipping-off

Guidance

1. Ancillary Service Providers are reminded that in accordance with Article 16 of the U.A.E. Law No. 4 of 2002 regarding Criminalisation of Money Laundering, Ancillary Service Providers or any of their Employees must not tip-off any Person, that is, inform any Person that his transaction is being scrutinised for possible involvement in suspicious Money Laundering operations, or that any other competent authority is investigating his possible involvement in suspicious Money Laundering operations.
2. If an Ancillary Service Provider reasonably believes that performing the 'Know Your Customer' process will tip-off a customer or potential customer, it may choose not to pursue that process and should file a Suspicious Transaction Report in accordance with Rule 6.6.2. Ancillary Service Providers should ensure that their Employees are aware of and sensitive to these issues when considering the 'Know Your Customer' process.

6.8 Government, regulatory and international findings

Guidance

1. Taking into account its risk assessment pursuant to section 6.9, an Ancillary Service Provider may make reference to and make appropriate use of any findings issued by:
 - a. the government of the U.A.E. or any government departments in the U.A.E.;
 - b. the Central Bank of the U.A.E. or the AMLSCU;
 - c. the Financial Action Task Force (FATF); and
 - d. the DFSA;which contain:
 - e. a finding or other conclusion concerning arrangements for restraining money laundering in a particular country or jurisdiction; and
 - f. an assessment that those arrangements assessed to be materially deficient in comparison with one or more of the relevant, internationally accepted standards, including any recommendations published by the FATF, required of or recommended to countries and jurisdictions.
2. When an Ancillary Service Provider makes a decision about its anti money laundering policies, procedures, systems and controls, it may take into account any findings of inadequacy, for example from the FATF list of Non Cooperative Countries and Territories, concerning the approach to money laundering of individual countries or jurisdictions.
3. Ancillary Service Providers should examine and pay special attention to any transactions or business relations with Persons located in such countries or jurisdictions.
4. Ancillary Service Providers considering transactions or business relationships with Persons located in countries or jurisdictions that have been identified as deficient, or against which the U.A.E. or the DFSA 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 introduced business from such jurisdictions, and when receiving inward payments for existing customers.
5. The Ancillary Service Provider's AMLO is not obliged to report all transactions from these countries or jurisdictions to the AMLSCU (if appropriate) and the DFSA if they do not qualify as suspicious pursuant to U.A.E Law No. 4.
6. Transactions with counterparties located in countries or jurisdictions which have been relieved from special scrutiny, for example taken off the FATF list of NCCTs, may nevertheless require attention which is higher than normal.

7. In order to assist Ancillary Service Providers, the DFSA will, from time to time, publish U.A.E. national, FATF or other findings. However, the DFSA expects that an Ancillary Service Provider takes its own steps in acquiring relevant information from various available sources.
8. Taking into account its risk assessment pursuant to section 6.9, an Ancillary Service Provider may make reference to and make appropriate use of any findings issued by:
 - a. the government of the U.A.E. or any government departments in the U.A.E.;
 - b. the Central Bank of the U.A.E. or the AMLSCU;
 - c. U.A.E. enforcement agencies; and
 - d. the DFSA;

which contain a finding or other conclusion concerning names of Persons, groups, organisations or entities or any other body where suspicion of Money Laundering or terrorist financing exists.
9. An Ancillary Service Provider may obtain and appropriately use available national and international information, for example suspect lists or databases from credible public or private sources with regard to Money Laundering and terrorist financing. The DFSA encourages Ancillary Service Providers 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.
10. The risk of terrorists entering the financial system can be reduced if Ancillary Service Providers apply effective anti money laundering strategies, particularly in respect of 'Know Your Customer' procedures, see Rules under sections 6.5 and 6.9 in conjunction with App2 and App3.

6.9 Money laundering risks

Risk assessment

- 6.9.1**
- (1) The anti money laundering policies, procedures, systems and controls of an Ancillary Service Provider must adequately address the money laundering risks which take into account any vulnerabilities of its products, services and customers.
 - (2) In assessing the risks in relation to money laundering, an Ancillary Service Provider must have regard to the relevant provisions of App2 and App3.
 - (3) An Ancillary Service Provider must assess its risks in relation to money laundering and perform enhanced due diligence investigations for higher risk products, services and customers.

- (4) An Ancillary Service Provider must be aware of any money laundering risks that may arise from new or developing technologies that might favour anonymity and take measures to prevent their use for the purpose of money laundering.

Risks regarding corruption and politically exposed persons

- 6.9.2** (1) An Ancillary Service Provider must have systems and controls to determine whether a customer is a Politically Exposed Person.
- (2) When an Ancillary Service Provider has a customer relationship with a Politically Exposed Person, it must have specific arrangements to address the risks associated with corruption and Politically Exposed Persons.

Guidance

Guidance on how an Ancillary Service Provider may address this risk is set out in App3 section A3.2.

Suspicious transactions and transaction monitoring

- 6.9.3** An Ancillary Service Provider must establish and maintain policies, procedures, systems and controls in order to monitor for and detect suspicious transactions.

Guidance

1. An Ancillary Service Provider should apply an intensified and ongoing monitoring programme over higher risk transactions and accounts.
2. Various risk aspects about transaction monitoring and about the detection of suspicious transactions, which the Ancillary Service Provider should take into account, are set out as further Guidance in App3 section A.3.3.

6.10 Awareness and training

- 6.10.1** An Ancillary Service Provider must have arrangements to provide periodic information and training to all relevant Employees to ensure that they are aware of:

- (a) the identity and responsibilities of the Ancillary Service Provider's AMLO;
- (b) applicable legislation relating to anti money laundering;
- (c) the potential effect on the Ancillary Service Provider, its Employees and its customers of breaches of applicable legislation relating to money laundering;
- (d) the Ancillary Service Provider's anti money laundering policies, procedures, systems and controls and any changes to these;

- (e) money laundering risks, trends and techniques;
- (f) the types of activity that may constitute suspicious activity in the context of the business in which an Employee is engaged that may warrant an internal Suspicious Transaction Report pursuant to Rule 6.6.1;
- (g) Ancillary Service Provider's arrangements regarding the making of an internal Suspicious Transaction Report pursuant to Rule 6.6.1;
- (h) the use of findings; and
- (i) customer identification requirements pursuant to the Rules in section 6.5.

6.10.2 Information described under Rule 6.10.1 must be brought to the attention of relevant new Employees and must remain available to all relevant Employees.

6.10.3 (1) An Ancillary Service Provider must have arrangements to ensure that:

- (a) its anti money laundering training is up-to-date with money laundering trends and techniques;
- (b) its anti money laundering training is appropriately tailored to the Ancillary Service Provider's different activities, services, customers and indicates any different levels of money laundering risk and vulnerabilities; and
- (c) all relevant Employees receive anti money laundering training.

(2) An Ancillary Service Provider must conduct anti money laundering training sessions with sufficient frequency to ensure that within 12 months it is provided to all relevant Employees.

6.10.4 (1) All relevant details of the Ancillary Service Provider's anti money laundering 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.

(2) These records must be kept for at least six years from the date on which he training was given.



APP1 [DELETED] [VER6/12-07] [RM52/07]

APP2 CUSTOMER IDENTIFICATION REQUIREMENTS

A2.1 Duties and responsibilities

Guidance relating to Rules 6.5.1 and 6.5.2

1. Pursuant to Rule 6.5.1, an Ancillary Service Provider is required to be satisfied that a prospective customer is who he claims to be and obtain evidence to prove this.
2. ‘Know your Customer’ and knowing the Persons with or for whom the customer acts or proposes to act, pursuant to Rule 6.5.2 consists of several aspects:
 - a. personal details: an Ancillary Service Provider should obtain and verify details which include the true full name or names used and the current permanent address;
 - b. the nature and level of business to be conducted: an Ancillary Service Provider should ensure that sufficient information is obtained regarding the nature of the business that the customer expects to undertake, and any expected or predictable pattern of transactions. This information should include the purpose and reason for establishing the business relationship, the anticipated level and nature of the activity that is to be undertaken;
 - c. the origin of funds: an Ancillary Service Provider should identify how all payments were made, from where and by whom. All payments should be recorded to provide an audit trail; and
 - d. the source of wealth: an Ancillary Service Provider should establish a source of wealth or income, including how the funds were acquired, to assess whether the actual transaction pattern is consistent with the expected transaction pattern and whether this constitutes any grounds for suspicion of money laundering.
3. It is important for an Ancillary Service Provider to obtain such information because this process should allow for the risk of being exploited for the purpose of money laundering to be reduced to a minimum. It should also enable suspicious transactions to be detected because they are incompatible with the information received.
4. Any unusual facts of which an Ancillary Service Provider becomes aware during the identification process may be an indication of money laundering and should prompt the Ancillary Service Provider to request supplementary information and evidence.
5. The DFSA expects an Ancillary Service Provider to establish the full identity of all relevant parties to the business relationship. Further, an Ancillary Service Provider should apply adequate measures to understand the relationship between the counterparties involved.

A2.2 Establishing identity – identification procedures

Guidance relating to Rules under section 6.5

1. In accordance with Rules 6.5.1 and 6.5.2, an Ancillary Service Provider is expected to establish to its satisfaction the true identity of a customer and any other Person on whose behalf the customer is acting, including that of the Beneficial Owner of the relevant funds which may be the subject of a transaction to be considered. The Ancillary Service Provider should verify that it is dealing with a true and existing Person. It also should obtain evidence of verification that is sufficient to establish that the Person is indeed who he claims to be.
2. The following list, which is not meant to be exhaustive, should be considered as Guidance regarding the type of information and evidence which should be obtained by an Ancillary Service Provider to establish and verify the identity of a customer.

Individuals

- a. Evidence to be obtained in either documentary (hard copy) or electronic form:
 - i. true full name or names used;
 - ii. complete current permanent address, including all relevant details with regard to country of residence;
 - iii. telephone, fax number and email address;
 - iv. date and place of birth;
 - v. nationality;
 - vi. fiscal residence;
 - vii. occupation or profession, name of employer and location of activity;
 - viii. information regarding the nature of the business to be conducted;
 - ix. information regarding the origin of the funds; and
 - x. information regarding the source of wealth or income.
- b. The address of a prospective customer should enable an Ancillary Service Provider to physically locate the customer. If P.O. Box numbers are customary to a country, additional methods of physically locating the customer should be applied.
- c. Documentary evidence of identity:
 - i. current, signed passport;
 - ii. current, signed ID card; or
 - iii. other identification documentation that is customary in the country of residence, such as driving licence, including a clear photograph of the prospective customer.
- d. An Ancillary Service Provider should ensure that any documents used for the purpose of identification are original documents.

- e. Where personal identity documents, such as passport, ID card or other identification documentation cannot be obtained in original form, for example because an Ancillary Service Provider has no physical contact with the customer the identification documentation provided should be certified as a true copy of the original document by any one of the following:
 - i. a registered lawyer;
 - ii. a registered notary;
 - iii. a chartered accountant;
 - iv. a government ministry;
 - v. a post office;
 - vi. a police officer; or
 - vii. an embassy or consulate.
- f. The individual or authority undertaking the certification under (e) should be contactable if necessary.
- g. Where a copy of an original identification document is made by an Ancillary Service Provider, the copy should be dated, signed and marked with 'original sighted'.
- h. Documentary evidence of address:
 - i. record of home visit;
 - ii. confirmation from an electoral register search that a Person of such a name lives at that address;
 - iii. tenancy agreement;
 - iv. utility bill; or
 - v. local authority tax bill.

Unincorporated businesses or partnerships

- i. Evidence to be obtained in either documentary or electronic form:
 - i. true full name or names;
 - ii. complete current registered and trading address, including relevant details with regard to country of establishment;
 - iii. telephone, fax number and email address;
 - iv. fiscal residence;
 - v. business activity;
 - vi. information on the nature of the business to be conducted;
 - vii. trading licence, with renewal date;
 - viii. list of authorised signatories of the business or partnership;
 - ix. regulatory body, if applicable;
 - x. information regarding the origin of funds; and
 - xi. information regarding the source of wealth/income.

- j. Documentary evidence of identity:
 - i. latest annual report and accounts, audited where applicable, and
 - ii. certified copy of the partnership deed, to ensure that it has a legitimate purpose and to ascertain the nature of the business or partnership.
- k. Evidence of the trading address of the business or partnership should be obtained and may be verified with a visit to the place of business.

Corporate entities including financial or credit institutions that are not covered by an exemption, including financial or credit institutions that are not regulated by the DFSA or regulated in a FATF country

- l. Evidence to be obtained in either documentary or electronic form:
 - i. registered corporate name and any trading names used;
 - ii. complete current registered address and any separate principal trading addresses, including all relevant details with regard to country of residence;
 - iii. telephone, fax number and email address;
 - iv. date and place of incorporation;
 - v. corporate registration number;
 - vi. fiscal residence;
 - vii. business activity;
 - viii. regulatory body, if applicable;
 - ix. name and address of group, if applicable;
 - x. legal form;
 - xi. name of external auditor;
 - xii. information regarding the nature and level of the business to be conducted;
 - xiii. information regarding the origin of the funds; and
 - xiv. information regarding the source of wealth/income.
- m. Documentary evidence of identity:
 - i. copy of the extract of the register of the regulator or exchange, or state law or edict creating the entity, in case of regulated, listed or state-owned companies;
 - ii. certified copy of the articles of association or statutes;
 - iii. certified copy of either the certificate of incorporation or the trade register entry and the trading licence including the renewal date;
 - iv. latest annual report, audited and published if applicable;
 - v. certified copies of the list of authorised signatories specifying who is authorised to act on behalf of the customer account and of the board resolution authorising the signatories to operate the account;
 - vi. certified copies of the identification documentation of the authorised signatories;
 - vii. names, country of residence, nationality of directors or partners and of the members of the governing body; and
 - viii. list of the main shareholders holding more than 5% of the issued capital.
- n. If the applying customer is not obliged to publish an audited annual report, adequate information about the financial accounts should be obtained.

- o. An Ancillary Service Provider should verify that the applying customer is active and has not been, or is not in the process of being dissolved, wound-up or terminated.

Trusts, nominees and fiduciaries

- p. In addition to the identification documentation listed under ‘corporate entities’ (l-m), the following information and documentation should be obtained:
 - i. identity of any settler, the trustee and any principal controller who has the power to remove the trustee as well as the identity of the Beneficial Owner;
 - ii. a certified copy of the trust deed, to ascertain the nature and purpose of the trust; and
 - iii. documentary evidence of the appointment of the current trustees.
- q. An Ancillary Service Provider should ensure that it is advised about any changes concerning the individuals who have control over the funds, and concerning the Beneficial Owners.
- r. Where a trustee, principal controller or Beneficial Owner who has been identified is about to be replaced, the identity of the new trustee, principal controller or Beneficial Owner should be verified before they are allowed to exercise control over the funds.

Authorised Firms, Ancillary Service Providers and Authorised Market Institutions regulated by the DFSA or financial or credit institutions regulated in a FATF country.

- s. Pursuant to Rule 6.5.5, identification evidence is generally not required for customers of a firm who are Authorised Firms, Ancillary Service Providers or Authorised Market Institutions registered or regulated by the DFSA.
- t. However, the confirmation of the existence of such a relevant firm or institution under Guidance note 2.s. above, its regulatory status, including the application of Rules applying in the DIFC or equivalent anti money laundering provisions, should be verified by the Ancillary Service Provider prior to entering into a customer relationship. Regular professional and commercial checks and due diligence investigations should still be performed. The Ancillary Service Provider should verify the regulatory status of the firm or institution by one of the following means:
 - i. request confirmation from the relevant Financial Services Regulator or other relevant regulatory authority, body, or home country Central Bank;
or
 - ii. request a certified copy of a relevant licence or authorisation to conduct financial or banking business from the firm or institution.

Clubs, cooperative, charitable, social or professional societies

- u. An Ancillary Service Provider should take steps to satisfy itself as to the legitimate purpose of clubs and societies by, for example, obtaining a certified copy of the constitution of the organisation.
 - v. The identity of the principal signatories and controllers should be verified in accordance with the requirements for private individuals. The capacity of the signatories to act on behalf of the club or society and the identity of Beneficial Owners of the funds should be established and verified.
 - w. An Ancillary Service Provider should consider the following items while completing the customer identification requirements for a client which is a charitable organisation:
 - i. Whether the charity is licensed or permitted by a regulatory authority or government entity in its home country (Note: charities in the UAE are required to obtain a certificate issued by the UAE Minister of Labour and Social Affairs which specifically allows for the opening of bank accounts).
 - ii. The type and quality of regulation to which the charity is subject in its home state.
 - iii. The structure and overall character of management and trustees.
 - iv. Whether the charity allows donors to specify beneficiaries. If yes, then it would be prudent to ascertain that such charities are closely regulated.
 - v. The pattern of beneficiaries - a small number of targeted beneficiaries could indicate potential risks.
 - vi. Whether the charity and its functioning is dominated by a few large donors and the pattern of donors.
 - vii. Whether it is a private foundation as it is more likely to be dominated by a single donor and linked to a small number of beneficiaries which will necessitate scrutiny of both the donor and the beneficiaries.
- [Added][VER5/06/07][RM43/07]
3. The DFSA will from time to time:
 - a. review the Guidance under App2 in light of changing money laundering legislation issued by the U.A.E. Central Bank, money laundering trends and techniques and according to international standards, in order to keep the Guidance current; and
 - b. provide such other Guidance as it deems appropriate regarding customer identification obligations.
 - c. The DFSA expects that an Ancillary Service Provider will take these changes into account by amending, as appropriate, its policies, procedures, systems and controls.
 4. Sound 'Know Your Customer' arrangements have particular relevance to the safety and soundness of an Ancillary Service Provider, in that:
 - a. they help to protect its reputation and the integrity of the DIFC by reducing the likelihood of Ancillary Service Providers becoming a vehicle for, or a victim of, financial crime and suffering consequential reputational damage; and

- b. they constitute an essential part of sound risk management.
- 5. Any inadequacy of 'Know Your Customer' standards can expose Ancillary Service Providers to serious business operation and control risks.
- 6. In accordance with Rule 6.5.1, an Ancillary Service Provider should adopt a risk-based approach for the customer identification and verification process. Depending on the money laundering risk assessment regarding the Ancillary Service Provider's customer, the Ancillary Service Provider should decide to what level of detail the customer identification and verification process will need to be performed. See also Rules under section 6.9. The risk assessment regarding a customer should be recorded in the customer file.
- 7. The risk-based approach does not release an Ancillary Service Provider from its overall obligation to identify fully and obtain evidence of customer identification to the DFSA's satisfaction.
- 8. An Ancillary Service Provider is advised that in cases of doubt it should adopt a stricter rather than a moderate approach in its judgement concerning the risk level and the level of detail to which customer identification is performed and evidence obtained.

APP3 MONEY LAUNDERING RISKS

A3.1 Risk assessment

Guidance relating to Rule 6.9.1

1. Generally, an Ancillary Service Provider is expected to take a risk-based approach when assessing any business relationship or transaction with respect to its specific money laundering risk and the information and evidence that might be required or validated for this purpose. 'Know Your Customer' procedures need to be established and managed according to the perceived money laundering risk.
2.
 - a. The Ancillary Service Provider should take specific and adequate measures necessary to compensate for the higher risk of money laundering which might arise, for example from the following products, services or customers:
 - i. non face-to-face business relationships or transactions, such as via mail, telephone or the Internet;
 - ii. customers from FATF 'Non Cooperative Countries and Territories' and higher-risk countries, see also Guidance under section 6.8; and
 - iii. Politically Exposed Persons, see also Rule 6.9.2.
 - b. Pursuant to Rule 6.9.3, an Ancillary Service Provider should apply an intensified monitoring of transactions and accounts in relation to these products, services and customers.
3. While an Ancillary Service Provider should assess the money laundering risks posed by the products and services it offers and devise its products with due regard to those risks, a risk-based approach does not release the Ancillary Service Provider from its overall obligation to comply with anti money laundering obligations.
4. The highest risk products or services in respect of money laundering are those where unlimited third party funds can be freely received, or where funds can regularly be paid to third parties, without evidence of identity of the third parties being taken.
5. Money laundering risks are increased if a Person is able to hide behind corporate structures such as limited companies, offshore trusts, special purpose vehicles and nominee arrangements. When devising its internal procedures, an Ancillary Service Provider should consider how its customers and operational systems impact upon the capacity of its staff to identify suspicious transactions.
6. The geographical location of an Ancillary Service Provider's customer may also affect the money laundering risk assessment. The DFSA recommends that where an Ancillary Service Provider has customers located in countries:
 - a. without adequate anti money laundering strategies;
 - b. where cash is the normal medium of exchange;
 - c. which have a politically unstable regime with high levels of public or private sector corruption;

- d. which are known to be drug producing or drug transit countries; or
- e. which have been classified as countries with inadequacies in their anti money laundering regulations, see Guidance under section 6.8;

it should consider which additional 'Know Your Customer' and monitoring procedures might be necessary to compensate for the enhanced risks of money laundering.

- 7. Such measures may encompass, for example, the following:
 - a. requiring additional documentary evidence;
 - b. taking supplementary measures to verify or certify the documents supplied; or
 - c. requiring that the initial transaction is carried out through an account opened in the customer's name with a credit or financial institution subject to these Rules or regulated in a FATF Country.

A3.2 Risks regarding corruption and politically exposed persons

Guidance relating to Rule 6.9.2

- 1. Corruption, especially with the involvement of Politically Exposed Persons, may involve serious crimes and has become the subject of increasing global concern. The risk for an Ancillary Service Provider can be reduced if the Ancillary Service Provider conducts detailed 'Know Your Customer' investigations at the beginning of a relationship and on an ongoing basis where it knows, suspects, or is advised that, the business relationship involves a Politically Exposed Person. An Ancillary Service Provider should develop and maintain enhanced scrutiny and monitoring practices to address this risk, see also App2.
- 2. Where a customer relationship is maintained with a PEP, detailed monitoring and due diligence procedures should include:
 - a. analysis of any complex structures, for example involving trusts or multiple jurisdictions;
 - b. appropriate measures to establish the source of wealth;
 - c. development of a profile of expected activity for the business relationship in order to provide a basis for transaction and account monitoring;
 - d. senior management approval for the customer relationship; and
 - e. regular oversight of the relationship with a Politically Exposed Person by senior management.
- 3. An Ancillary Service Provider is advised that customer relationships with family members or close associates of Politically Exposed Persons involve similar risks to those with Politically Exposed Persons themselves.

A3.3 Suspicious transactions and transaction monitoring

Guidance relating to Rule 6.9.3

1. a. The Rules in section 6.6 require a Suspicious Transaction Report to be made when there is knowledge or suspicion of money laundering. Suspicion is a personal and subjective assessment. Suspicion of money laundering requires a degree of satisfaction although this may not amount to belief, it should at least extend beyond mere speculation and should be based upon some foundation that money laundering has or is about to occur.
- b. A member of staff who considers a transaction 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.
- c. The Rules in section 6.6 also make reference to 'reasonable grounds to suspect' which introduces an objective test rather than a subjective test of suspicion by assessing whether or not 'suspicion' was ignored in the way of:
 - i. wilful blindness;
 - ii. negligence, that is wilfully and recklessly failing to make the adequate enquiries; or
 - iii. failing to assess adequately the facts and information that are either presented or available.
2. a. 'Know Your Customer' requirements form the basis for recognising suspicious transactions, see Rules under section 6.5 and App2. Sufficient guidance must therefore be given to the Ancillary Service Provider's Employees to enable them to form a suspicion or to recognise when they have reasonable grounds to suspect that money laundering 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 transaction is suspicious in the circumstances, see Rules under section 6.9.
- b. Effective 'Know Your Customer' arrangements may provide the basis for recognising unusual and suspicious transactions. Where there is a customer relationship, a suspicious transaction will often be one that is inconsistent with a customer's known legitimate transactions, or with the normal business activities for that type of account or customer. Therefore, the key to recognising 'suspicions' is knowing enough about the customer and the customer's normal expected activities to recognise when a transaction is abnormal. Circumstances that might give rise to suspicion or reasonable grounds for suspicion may be:
 - i. transactions which have no apparent purpose and which make no obvious economic sense;
 - ii. transactions requested by a customer without reasonable explanation, which are out of the ordinary range of services normally requested or are outside the experience of an Ancillary Service Provider in relation to a particular customer;
 - iii. the size or pattern of transactions, without reasonable explanation, is out of line with any pattern that has previously emerged;
 - iv. a customer refuses to provide the information requested without reasonable explanation;
 - v. a customer who has just entered into a customer relationship uses the relationship for a single transaction or for only a very short period of time;

- vi. an extensive use of offshore accounts, companies or structures in circumstances where the customer's economic needs do not support such requirements;
 - vii. unnecessary routing of funds through third party accounts; or
 - viii. unusual transactions without an apparently profitable motive.
3. Pursuant to Rule 6.9.3, an Ancillary Service Provider is required to have transaction monitoring policies, procedures, systems and controls. On going monitoring of customer activity, that is, monitoring of transactions and their accounts, either through manual procedures or by computerised systems, is one of the most important aspects of effective 'Know Your Customer' processes. Whether an Ancillary Service Provider should undertake the monitoring by means of a manual or computerised system will depend on a number of factors, including, but not limited to, the Ancillary Service Provider's:
 - a. size and nature of the business and customer base;
 - b. complexity of the transactions; and
 - c. volume of the transactions.
4. The extent of 'Know Your Customer' information and that of required transaction monitoring should be assessed taking a risk-based approach. Higher risk accounts and customer relationships will generally require more frequent or detailed monitoring.