Appendix 2

The text in this appendix is new and is not underlined and struck through in the usual manner.

The DFSA Rulebook

Designated Non-Financial Businesses and Professions Module

(DNF)

Contents

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

1 INTRODUCTION

1.1 Application

1.1.1 (1) This module (DNF) 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 DNF provides for a narrower application.

(2) Chapters 1 to 4 apply to every DNFBP.

(3) Chapter 5 applies to every DNFBP other than a Single Family Office.

(4) Chapter 6 applies only to a DNFBP which is a Single Family Office.

(5) DNF also applies to a Person in his capacity as the MLRO of a DNFBP appointed in accordance with Chapter 4.

1.2 Interpretation

1.2.1 In relation to a Single Family Office references in this module to "customer" are to be read as meaning a Single Family (as defined under the DIFCA Single Family Office Regulations) to whom the Single Family Office provides a service.

Guidance

1. Every provision in the DNF 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 DNF 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 form include the plural and words in the plural form 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.

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.

2 DEFINITION OF NON-FINANCIAL BUSINESSES AND PROFESSIONS

Guidance

Pursuant to Rule 1.1.1(2) this Chapter applies to every DNFBP.

2.1 Definition

2.1.1 (1) For the purposes of Article 60(6) of the Law, the DFSA hereby prescribes, subject to (2), the following Persons to be a DNFBP:

(a) Real estate developers and agents which carry out transactions with a customer which concern the buying or selling of real property;

(b) Dealers in precious metals and dealers in precious stones which engage in any cash transaction with a customer equal to or above fifteen thousand dollars ($15,000);

(c) Dealers in high-value goods which engage in any cash transaction with a customer equal to or above fifteen thousand dollars ($15,000);

(d) Law firms, notary firms, other independent legal businesses and accounting, audit and insolvency firms which prepare or carry out transactions for a customer of the following kind:

(i) buying and selling of real estate;

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

(iii) managing of bank, savings or securities accounts;

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

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

(e) company service providers which carry out any of the following activities for a customer:

(i) acting as a formation agent of legal persons;

(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;

(iii) providing a registered office; business address or accommodation, correspondence or administrative address for

a company, a partnership or any other legal person or arrangement; or

(iv) acting as (or arranging for another person to act as) a nominee shareholder for another person, and

(f) Single Family Offices,

whose business or profession is carried on in or from the DIFC.

(2) A Person who is an Authorised Firm or an Ancillary Service Provider is not a DNFBP.

2.1.2 In Rule 2.3.2(1) (b) and (c), a transaction meets the designated threshold of fifteen thousand dollars ($15,000) whether it is executed as a single operation or in several connected operations.

Guidance

The Financial Action Task Force (FATF) is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. The United Arab Emirates (UAE) is a member of the Gulf Cooperation Council (GCC), which in turn is a member of the Financial Action Task Force (FATF). The UAE is also a member of the regional body for the AML/CTF in the Middle East and North Africa (MENAFATF). The UAE commits to comply with the measures agreed to by the FATF members, in particular, to comply with the FATF Forty Recommendations and Nine Special Recommendations, which includes three recommendations which specifically address DNFBPs.

3 REGULATORY PROCESSES

3.1 Registration by notification to the DFSA

3.1.1 A DNFBP must register with the DFSA by way of a notification by completing and submitting the appropriate form in AFN.

3.1.2 A DNFBP must promptly notify the DFSA of any change in its:

(a) name;

(b) legal status; or

(c) address.

3.1.3 A DNFBP must notify the DFSA when it proposes to cease carrying on the business activity or activities listed in Rule 2.1.2 by completing and submitting the appropriate form in AFN.

3.2 Co-operation with regulators

3.2.1 A DNFBP must promptly inform the DFSA in writing if it receives a request for information from a regulator or agency responsible for anti money laundering regarding enquiries into potential money laundering related to its activities carried on in or from the DIFC.

3.3 Communication with the DFSA

3.3.1 A DNFPB must ensure that any communication with the DFSA is conducted in the English language.

3.2 Supervision and enforcement powers

Guidance

1. A DNFBP should ensure that it complies with and has regard to relevant provisions of the Regulatory Law 2004. The Regulatory Law 2004 gives the DFSA a power to supervise DNFBPs' compliance with relevant anti-money laundering laws in the UAE. It also gives the DFSA a number of other important powers in relation to DNFBPs including powers of supervision and enforcement. These include powers to obtain information and to conduct investigations into possible breaches of the Regulatory Law 2004. The DFSA may also impose fines for breaches of the Law or the Rules.

2. The DFSA takes a risk-based approach to regulation of Persons which it supervises. Generally, the DFSA will work with DNFBPs to identify, assess, mitigate and control relevant risks where appropriate. ENF describes the DFSA's enforcement powers under the Regulatory Law 2004 and outlines its policy for using these powers. ENF also establishes the framework for the DFSA's decision making process and the giving of notices in relation to enforcement powers.

4 GENERAL PROVISIONS

Guidance

1. Pursuant to Rule 1.1.1(2), this chapter applies to every DNFBP.

2. The Rules in this Module require DNFBPs 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.

3. Accordingly, where the DFSA uses the term 'money laundering', DNFBPs 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.

4.1 General requirements

4.1.1 (1) A DNFBP must establish and maintain effective anti money laundering policies, procedures, systems and controls to prevent opportunities for Money Laundering in relation to the DNFBP and its activities.

(2) A DNFBP 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. A DNFBP's anti money laundering policies, procedures, systems and controls should:

   a. ensure compliance with the 'Federal Law No. 4 of 2002 - Criminalisation of Money Laundering of the U.A.E.' (U.A.E. Law No.4), the 'Federal Law No. 1 of 2004' regarding anti-terrorism and any other relevant Federal laws;

   b. enable suspicious customers and transactions to be detected and reported;

   c. ensure the DNFBP is able to provide an audit trail of a transaction; and

   d. comply with any other obligation in these Rules.

2. A DNFBP'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. A DNFBP should have a policy statement detailing the duties and obligations of its MLRO.

4. A DNFBP 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, a DNFBP may be criminally liable for the offence of Money Laundering if such an activity is intentionally committed in its names or for its accounts.

4.1.2 If another jurisdiction's legislation prevents or inhibits a DNFBP from complying with the U.A.E. Law No.4 or with these Rules, the DNFBP must promptly inform the DFSA in writing.

4.2 Appointment of an MLRO

Appointment

4.2.1 (1) A DNFBP must, as soon as reasonably practicable, designate an individual within the DNFBP to be its Money Laundering Reporting Officer (MLRO).

(2) A DNFBP must notify the DFSA of the appointment of its MLRO by completing and filing with the DFSA the appropriate form in AFN.

4.2.2 A DNFBP must ensure that the MLRO is of sufficient seniority within the DNFBP 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 DNFBP 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 DNFBP has entered into or may have contemplated entering into with or for the customer or that Person.

4.2.3 If the MLRO leaves the employment of the relevant DNFBP, the DNFBP must designate a successor within 28 days.

4.2.4 A DNFBP may outsource its MLRO function to an individual outside the DNFBP provided that the relevant service provider under the outsourcing agreement is and remains suitable to perform the MLRO function.

Guidance

Notwithstanding any outsourcing under Rule 4.2.4, a DNFBP remains responsible for compliance with the DNF Module.

4.3 Relevant United Nations Resolutions and Sanctions

4.3.1 (1) A DNFBP must establish and maintain effective systems and controls to:

(a) obtain and make appropriate use of relevant resolutions or sanctions issued by the United Nations Security Council; and

(b) disclose in its annual MLRO report the manner in which it has complied with such relevant resolutions or sanctions.

(2) In relation to an activity which is restricted or prohibited by a relevant sanction or resolution issued by the United Nations Security Council, a DNFBP must immediately notify the DFSA when it becomes aware that it is:

(a) carrying on or about to carry on a service;

(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) and (b);

for or on behalf of a Person, and such carrying on, holding or undertaking constitutes or may constitute a contravention of a relevant sanction or resolution issued by the United Nations Security Council.

(3) A DNFBP must ensure that the notification stipulated in (2) above includes the following information:

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

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

Guidance

1. In relation to the term "make appropriate use" in Rule 4.3.1, this may mean that a DFNBP cannot undertake a transaction for or on behalf of a Person or that it may need to undertake further due diligence in respect of a Person.

2. Relevant resolutions or sanctions mentioned in Rule 4.3.1 may, inter alia, relate to money laundering or terrorist financing or financing of weapons of mass destruction or otherwise may be relevant to the services provided by, or business activities of, the DNFBP. For example, a DNFBP should exercise due care to ensure that it does not provide any service to a Person engaged in money laundering or terrorist financing or financing of weapons of mass destruction.

3. In respect of the United Nations Security Council's resolutions or sanctions, the MLRO should also refer to Rules 5.1.1(2)(i), 5.1.2(e) and 5.6.1(h) for requirements relating to the MLRO's responsibility, reporting and training and awareness.

4.4 Government, regulatory and international findings

4.4.1 A DNFBP must establish and maintain systems and controls to obtain and make appropriate use of any findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions 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;

concerning arrangements for preventing money laundering and terrorist financing in a particular country or jurisdiction, including any assessment of material deficiency against relevant countries in adopting international standards.

Guidance

1. The systems and controls mentioned in Rule 4.4.1 should be established and maintained by a DNFBP taking into account its risk assessment pursuant to section 5.5 or 6.2. In relation to the term "make appropriate use" in Rule 4.4.1, this may mean that a DNFBP cannot undertake a transaction for or on behalf of a Person or that it may need to undertake further due diligence in respect of a Person.

2. When a DNFBP makes a decision about its anti money laundering policies, procedures, systems and controls, it should take into account any findings of inadequacy, for example, any notice or guidance from the FATF concerning the approach to money laundering of individual countries or jurisdictions.

3. A DNFBP should examine and pay special attention to any transactions or business relations with Persons located in such countries or jurisdictions.

4. A DNFBP 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 assessment 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. A DNFBP's MLRO 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 sources mentioned in this Guidance, may nevertheless require attention which is higher than normal.

7. In order to assist DNFBPs, the DFSA will, from time to time, publish U.A.E. national, FATF or other findings, guidance, directives or sanctions. However, the DFSA expects a DNFBP to take its own steps in acquiring relevant information from various available sources. For example, a DNFBP may obtain relevant information from the consolidated list of financial sanctions in the European Union Office, HM Treasury (United Kingdom) lists, and the Office of Foreign Assets Control (OFAC) of the United States Department of Treasury.

8. DNFBPs should take note of Rule 4.3.1 which requires such service providers to obtain and make appropriate use of the United Nations Security Council's relevant resolutions and sanctions. Such resolutions and sanctions may, for example, relate to money laundering and terrorist financing and financing of weapons of mass destruction.

4.4.2 A DNFBP must establish and maintain systems and controls to obtain and make appropriate use of any findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions 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;

concerning names of Persons, groups, organisations or entities or any other body where suspicion of money laundering or terrorist financing exists.

Guidance

1. The systems and controls mentioned in Rule 4.4.2 should be established and maintained by a DNFBP taking into account its risk assessment pursuant to section 5.5 or 6.2. In relation to the term "make appropriate use" in Rule 4.4.2, this may mean that a DNFBP cannot undertake a transaction for or on behalf of a Person or that it may need to undertake further due diligence in respect of a Person.

2. A DNFBP 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 DNFBPs 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.

3. The risk of terrorists entering the financial system can be reduced if DNFBPs apply effective anti money laundering strategies, particularly in respect of 'Know Your Customer' procedures. See Rules under sections 5.2 or 6.2 in conjunction with App1 and App2.

4. DNFBPs should take note of Rule 4.3.1 which requires such service providers to obtain and make appropriate use of the United Nations Security Council's relevant resolutions and sanctions. Such resolutions and sanctions may, for example, relate to money laundering and terrorist financing and financing of weapons of mass destruction.

5 ANTI MONEY LAUNDERING RULES

Guidance

Pursuant to Rule 1.1.1(3), this Chapter applies to every DNFBP other than a Single Family Office.

5.1 Responsibilities of the MLRO

5.1.1 (1) A DNFBP must ensure that its MLRO is responsible for its anti money laundering activities carried on in or from the DIFC.

(2) A DNFBP must ensure that its MLRO carries out and is responsible for the following:

(a) establishing and maintaining the DNFBP'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 DNFBP's anti money laundering policies, procedures, systems and controls;

(c) acting as the point of contact to receive internal Suspicious Transaction Reports from the DNFBP's Employees pursuant to Rule 5.3.1;

(d) taking appropriate action pursuant to Rule 5.3.2 following the receipt of an internal Suspicious Transaction Report from the DNFBP'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 5.3.2;

(f) acting as the point of contact within the DNFBP 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;

(h) establishing and maintaining an appropriate anti money laundering training programme and adequate awareness arrangements pursuant to Rules under section 5.6; and

(i) receiving and acting upon relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions under Rules 4.3.1 to 4.4.2.

Reporting

5.1.2 The MLRO must report at least annually in writing to the Governing Body or senior management of the DNFBP on the following matters:

(a) the DNFBP's compliance with applicable anti money laundering laws including Rules;

(b) the quality of the DNFBP's anti money laundering policies, procedures, systems and controls;

(c) any internal Suspicious Transaction Reports made by the DNFBP's staff pursuant to Rule 5.3.1 and action taken in respect of those reports, including the grounds for all decisions;

(d) any external Suspicious Transaction Reports made by the DNFBP pursuant to Rule 5.3.2 and action taken in respect of those reports including the grounds for all decisions;

(e) any relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions under Rules 4.3.1 and 4.4.1 and how the DNFBP has taken them into account; and

(f) any other relevant matters related to money laundering as it concerns the DNFBP's business.

5.1.3 A DNFBP must ensure that its Governing Body or senior management promptly:

(a) assess the report provided under Rule 5.1.2;

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

(c) make a written record of their assessment in (a) and the action taken in (b).

5.1.4 The annual MLRO report in Rule 5.1.2 must be provided to the Governing Body or senior management of the DNFBP within 2 months of the DNFBP's financial year-end.

5.1.5 A DNFBP must provide a copy of each the documents in Rule 5.1.2 and 5.1.3(c) to the DFSA on request.

5.2 Customer identification requirements

Duties and responsibilities

5.2.1 (1) Subject to Rule 5.2.6, a DNFBP must establish and verify the identity of any customer with or for whom the DNFBP has acted, acts or proposes to act.

(2) In establishing and verifying a customer's true identity, a DNFBP must obtain sufficient and satisfactory evidence having considered:

(a) its risk assessment under Rule 5.5.1 in respect of the customer; and

(b) the relevant provisions of App1 and App2.

(3) A DNFBP must update as appropriate any customer identification policies, procedures, systems and controls.

Guidance

A DNFBP should adopt a risk-based approach for the customer identification and verification process. Depending on the outcome of the DNFBP'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.

5.2.2 Where Rule 5.2.1 applies to a DNFBP, it must, subject to Rule 5.2.6

(a) establish whether the customer is acting on his own behalf or on the behalf of another Person; and

(b) 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

A DNFBP 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 DNFBP obtains a written statement, confirming the statement made by the customer, from the parties including that of the Beneficial Owner.

5.2.3 A DNFBP must, subject to Rule 5.2.6, fulfil the obligations under Rules 5.2.1 and 5.2.2 prior to entering into a business relationship or transaction with a customer.

5.2.4 A DNFBP may fulfil the obligations under Rules 5.2.1 and 5.2.2 during the establishment of a business relationship if:

(a) it is necessary not to interrupt the normal conduct of business;

(b) there is little risk of money laundering or terrorist financing; and

(c) the relevant obligations are fulfilled as soon as practicable after contact is being established.

5.2.5 (1) A DNFBP must:

(a) ensure that the information and documentation concerning a customer's identity remains accurate and up-to-date; and

(b) conduct ongoing due diligence on its business relationship with, and ongoing scrutiny of transactions undertaken by, a customer throughout the course of the relationship.

(2) If at any time a DNFBP 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 evidence to verify the customer's identity.

Guidance

1. A DNFBP should undertake a periodic review to ensure that customer identity documentation is accurate and up-to-date.

2. When conducting ongoing due diligence on the business relationship with, and scrutiny of transactions undertaken by, a customer, a DNFBP should:

   a. ensure consistency of such transactions with its knowledge of the customer and the customer's intended purpose and the nature of the relationship; and

   b. verify, where necessary, the source of funds.

3. The degree of the ongoing due diligence to be undertaken will depend on the risk assessment carried out pursuant to section 5.5 including the nature of the business relationship and the type of product or service being provided.

Exception to customer identification requirements

5.2.6 (1) Subject to Rule 5.2.8, a DNFBP is not required to establish the identity of a customer pursuant to Rule 5.2.1 if the customer is one of the following:

(a) an Authorised Firm;

(b) an Authorised Market Institution; or

(c) an Ancillary Service Provider.

Guidance

The DFSA would expect a DNFBP 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.

5.2.7 Subject to Rule 5.2.8, a DNFBP is not required to establish the beneficial ownership pursuant to Rule 5.2.2 if the DNFBP's customer is a Person falling within Rule 5.2.6.

5.2.8 (1) Rules 5.2.6 and 5.2.7 do not apply where the DNFBP:

(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 DNFBP 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

5.2.9 (1) All relevant information, correspondence and documentation used by a DNFBP to:

(a) verify a customer's identity pursuant to Rules 5.2.1 and 5.2.2; and

(b) conduct the ongoing due diligence and scrutiny required under Rule 5.2.5,

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 a DNFBP should be kept in such a manner that:

a. the DFSA or another competent third party is able to assess the DNFBP's compliance with legislation applicable in the DIFC;

b. any transaction which was processed by or through the DNFBP 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 DNFBP can satisfy, within an appropriate time, any regulatory enquiry or court order to disclose information.

5.2.10 Where Rule 5.2.1 applies to a DNFBP, it must keep all relevant details of any transaction carried out with or for a customer for at least six years from the date on which the transaction was completed.

Reliance on others to verify identity

5.2.11 A DNFBP 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 DNFBP from any of its obligations under applicable laws including the Rules.

2. If the identification process has not been performed in accordance with these Rules, the DNFBP is expected to perform the identification process itself.

5.2.12 (1) Where a customer is introduced by another member of the DNFBP's Group, a DNFBP need not re-identify the customer, provided that:

(a) the identity of the customer has been verified by the other member of the DNFBP'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 DNFBP'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 DNFBP without delay; and

(iii) the identification evidence is kept for at least six years.

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

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

(2) A DNFBP must verify if there is secrecy or data protection legislation that would restrict access to such data by the DNFBP, the DFSA or the law enforcement agencies of the U.A.E. Where such legislation exists, the DNFBP 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.

5.2.14 A DNFBP 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 DNFBP.

5.3 Internal and external reporting requirements

5.3.1 (1) A DNFBP 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 DNFBP's MLRO.

(2) A DNFBP 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.

5.3.2 If a DNFBP's MLRO 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

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. A DNFBP may allow its Employees to consult with their line managers before sending a report to the MLRO. 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. DNFBPs 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.

5.3.3 The MLRO 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.

5.3.4 A DNFBP must keep all relevant details of any internal and external Suspicious Transaction Report made pursuant to Rules 5.3.1 and 5.3.2 for at least six years from the date on which the report was made.

5.3.5 A DNFBP must ensure that if the MLRO decides to make an external Suspicious Transaction Report in accordance with Rule 5.3.2, his decision is made independently and is not subject to the consent or approval of any other Person.

5.3.6 A DNFBP must not carry out a transaction which it knows or suspects, or has reasonable grounds for knowing or suspecting, is related to Money Laundering until it has informed the AMLSCU (if appropriate) and the DFSA pursuant to Rule 5.3.2.

Guidance

1. In preparation of an external Suspicious Transaction Report, if a DNFBP 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 DNFBP's proposed course of further action in relation to the case should be included in the report.

2. If the DNFBP has reported a suspicion to the AMLSCU, it may instruct the DNFBP on how to proceed with the transaction. If the customer in question expresses his wish to move the funds before a DNFBP receives instruction from the AMLSCU (if appropriate) on how to proceed, the DNFBP should immediately contact the AMLSCU for further instructions.

5.4 Tipping-off

Guidance

1. DNFBPs are reminded that in accordance with Article 16 of the U.A.E. Law No. 4 of 2002 regarding Criminalisation of Money Laundering, DNFBPs 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 a DNFBP 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 5.3.2. DNFBPs should ensure that their Employees are aware of and sensitive to these issues when considering the 'Know Your Customer' process.

5.5 Money laundering risks

Risk assessment

5.5.1 (1) The anti money laundering policies, procedures, systems and controls of a DNFBP 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, a DNFBP must have regard to the relevant provisions of App1 and App2.

(3) A DNFBP must assess its risks in relation to money laundering and perform enhanced due diligence investigations for higher risk products, services and customers.

(4) A DNFBP 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

5.5.2 (1) A DNFBP must have systems and controls to determine whether a customer is a Politically Exposed Person.

(2) When a DNFBP 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 a DNFBP may address the risks associated with corruption and politically exposed persons is set out in App2 section A2.2.

Suspicious transactions and transaction monitoring

5.5.3 A DNFBP must establish and maintain policies, procedures, systems and controls in order to monitor and detect suspicious transactions.

Guidance

1. A DNFBP 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 DNFBP should take into account, are set out as further Guidance in App2 section A.2.3.

5.6 Training and Awareness

5.6.1 A DNFBP 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 DNFBP's MLRO;

(b) applicable legislation relating to anti money laundering;

(c) the potential effect on the DNFBP, its Employees and its customers of breaches of applicable legislation relating to money laundering;

(d) the DNFBP'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 5.3.1;

(g) DNFBP's arrangements regarding the making of an internal Suspicious Transaction Report pursuant to Rule 5.3.1;

(h) the use of relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions described in Rules 4.3.1 and 4.4.1; and

(i) requirements relating to customer identification and ongoing due diligence of business relations and scrutiny pursuant to the Rules in section 5.2.

5.6.2 Information described under Rule 5.6.1 must be brought to the attention of relevant new Employees and must remain available to all relevant Employees.

5.6.3 (1) A DNFBP 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 DNFBP'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) A DNFBP must conduct anti money laundering training sessions with sufficient frequency to ensure that within 12 months it is provided to all relevant Employees.

5.6.4 (1) All relevant details of the DNFBP'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 the training was given.

6 ANTI MONEY LAUNDERING RULES FOR SINGLE FAMILY OFFICES

Guidance

1. Pursuant to Rule 1.1.1(4) this chapter applies only to a DNFBP which is a Single Family Office.

2. While Chapter 6 of DNF does not contain specific Rules on internal and external reporting requirements, a Single Family Office should be aware of the requirement to make a suspicious transaction report to the AMLSCU pursuant to either Federal Law No. 4 of 2002 or Federal Law No. 1 of 2004.

6.1 Responsibilities of the MLRO

6.1.1 (1) A Single Family Office must ensure that its MLRO is responsible for its anti money laundering activities carried on in or from the DIFC.

(2) A Single Family Office must ensure that its MLRO carries out and is responsible for the following:

(a) establishing and maintaining the Single Family Office'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 Single Family Office's anti money laundering policies, procedures, systems and controls;

(c) acting as the point of contact within the Single Family Office for competent U.A.E. authorities and the DFSA regarding money laundering issues;

(d) responding promptly to any request for information made by competent U.A.E. authorities or the DFSA; and

(e) receiving and acting upon relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other actions under Rules 4.3.1 to 4.4.2.

6.2 Customer due diligence requirements

Duties and responsibilities

6.2.1 A Single Family Office must establish and verify the identity of its customers.

6.2.2 The MLRO of a Single Family Office should, based on the outcome of a risk assessment, decide to what level of detail the identification and verification process in Rule 6.2.1 will need to be performed.

6.2.3 The MLRO of a Single Family Office must carry out the due diligence required by Rule 6.2.1 on a risk-sensitive basis and as follows:

6.2.4 (a) when identifying an individual, the MLRO must use a reliable source of identification information, and independent source documents, data or information;

(b) when identifying a trust or other similar entity, the MLRO must take reasonable steps to obtain information enabling him to understand the legal and beneficial ownership and control of the trust;

(c) when identifying other entities, the MLRO must take reasonable steps to understand the legal and beneficial ownership and control of the entity concerned; and

(d) when identifying a family businesses, the MLRO must take reasonable measures to understand the legal and beneficial ownership and control of the Family Business.

6.2.5 A Single Family Office must update as appropriate any customer identification policies, procedures, systems and controls.

Guidance

1. A Single Family Office should adopt a risk-based approach for the customer identification and verification process. Depending on the outcome of the Single Family Office'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.

2. In assessing the risks in relation to money laundering and in carrying out due diligence, a Single Family Office may be assisted by referring to the relevant guidance in App1 and App2.

3. A Single Family Office should 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.

4. The MLRO of a Single Family Office need not obtain identification data in relation to every customer who is an individual, but in order to understand issues of legal and beneficial ownership and control and in order to comply with the requirement to submit an SFO Annual Return he should consider (on a risk-sensitive basis) whether it is appropriate to obtain identification records in relation to any customer who:

i. is a settlor in relation to any fiduciary structure;

ii. acts as trustee, protector or enforcer of, or holds any fiduciary power in relation to, any trust or other similar entity or holds power to appoint or remove any trustee, protector or enforcer;

iii. is a director or alternate director of any Body Corporate which acts as trustee, protector or enforcer of, or holds any fiduciary powers in relation to, any trust or other similar entity;

iv. holds any power of appointment (whether general or special) or power of revocation or direction over the assets (or the income thereof) of a trust or other similar entity;

v. receives a benefit from, as a beneficiary of, any trust or other similar entity;

vi. is a director or alternate director or partner of, or otherwise controls, any entity or business; or

vii. is a Politically Exposed Person.

5. In relation to any customer which is a trust or other similar entity or business, the MLRO should obtain sufficient information to enable him to understand the nature of the customer's legal and beneficial ownership and control and how it relates to the Single Family. This may require the MLRO to obtain identification data about individuals who fall within the categories set out in Guidance note 4 (i) to (vii) above.

6.3 Record keeping

6.3.1 A Single Family Office must keep all relevant information, correspondence and documentation used to verify a customer's identity pursuant to Rule 6.2.1 for at least six years from the date on which the business relationship with a customer has ended.

APP1 CUSTOMER IDENTIFICATION REQUIREMENTS

A1.1 Duties and responsibilities

Guidance relating to Rules 5.2.1 and 5.2.2

1. Pursuant to Rule 5.2.1, a DNFBP 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 5.2.2 consists of several aspects:

   a. personal details: a DNFBP 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: a DNFBP 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: a DNFBP 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: a DNFBP 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 a DNFBP 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 a DNFBP becomes aware during the identification process may be an indication of money laundering and should prompt the DNFBP to request supplementary information and evidence.

5. The DFSA expects a DNFBP to establish the full identity of all relevant parties to the business relationship. Further, a DNFBP should apply adequate measures to understand the relationship between the counterparties involved.

A1.2 Establishing identity – identification procedures

Guidance relating to Rules under section 5.2

1. In accordance with Rules 5.2.1 and 5.2.2, a DNFBP 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 DNFBP 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 a DNFBP 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 a DNFBP 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. A DNFBP 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 a DNFBP 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 DNFBP, 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, and 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. A DNFBP 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 settlor, the trustee and any principal controller who has the power to remove the trustee(s) 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 trustee(s).

q. A DNFBP 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, DNFBPs and Authorised Market Institutions registered with or regulated by the DFSA or financial or credit institutions regulated in a FATF country.

s. Pursuant to Rule 5.2.6, identification evidence is generally not required for customers of a firm who are Authorised Firms, Ancillary Service Providers, DNFBPs 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 DNFBP prior to entering into a customer relationship. Regular professional and commercial checks and due diligence investigations should still be performed. The DNFBP 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. A DNFBP 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. A DNFBP 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.

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;

   b. provide such other Guidance as it deems appropriate regarding customer identification obligations; and

   c. The DFSA expects that a DNFBP 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 a DNFBP, in that:

   a. they help to protect its reputation and the integrity of the DIFC by reducing the likelihood of DNFBPs 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 DNFBPs to serious business operation and control risks.

6. In accordance with Rule 5.2.1, a DNFBP should adopt a risk-based approach for the customer identification and verification process. Depending on the money laundering risk assessment regarding the DNFBP's customer, the DNFBP should decide to what level of detail the customer identification and verification process will need to be performed. See also Rules under section 5.5. The risk assessment regarding a customer should be recorded in the customer file.

7. The risk-based approach does not release a DNFBP from its overall obligation to identify fully and obtain evidence of customer identification to the DFSA's satisfaction.

8. A DNFBP 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.

APP2 MONEY LAUNDERING RISKS

A2.1 Risk assessment

Guidance relating to Rule 5.5.1

1. Generally, a DNFBP 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 DNFBP 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 higher-risk countries, as may be found in sources mentioned in Guidance under Rule 4.4.1; and
   iii. Politically Exposed Persons, see also Rule 5.5.2.

   b. Pursuant to Rule 5.5.3, a DNFBP should apply an intensified monitoring of transactions and accounts in relation to these products, services and customers.

3. While a DNFBP 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 DNFBP 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, a DNFBP should consider how its customers and operational systems impact upon the capacity of its staff to identify suspicious transactions.

6. The geographical location of a DNFBP's customer may also affect the money laundering risk assessment. The DFSA recommends that where a DNFBP 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 Rule 4.4.1);

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 which is an Authorised Firm or which is regulated in a FATF Country.

A2.2 Risks regarding corruption and politically exposed persons

Guidance relating to Rule 5.5.2

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 a DNFBP can be reduced if the DNFBP 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. A DNFBP 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. A DNFBP 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.

A2.3 Suspicious transactions and transaction monitoring

Guidance relating to Rule 5.5.3

1. a. The Rules in section 5.3 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 5.3 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 5.2 and App1. Sufficient guidance must therefore be given to the DNFBP'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 5.5.

   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 a DNFBP 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 5.5.3, a DNFBP 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 a DNFBP should undertake the monitoring by means of a manual or computerised system will depend on a number of factors, including, but not limited to:

   a. the size and nature of the DNFBP's business and customer base; and

   b. the complexity and volume of the DNFBP's 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.