CAPITAL MARKET AUTHORITY

Anti-Money Laundering and Counter-Terrorist Financing Rules

English Translation of the Official Arabic Text

Issued by the Board of the Capital Market Authority

Pursuant to its Resolution Number (1-39-2008)

Dated 3/12/1429 H Corresponding to 1/12/2008

Based on the Capital Market Law

issued by Royal Decree No. M/30 dated 2/6/1424H

Amended by Resolution of the Board of the Capital Market Authority Number (5-53-2016) Dated 25/7/1437H Corresponding to 2/5/2016G

Arabic is the official language of the Capital Market Authority

The current version of these Regulations, as may be amended, can be found at the CMA website: www.cma.org.sa

Anti-Money Laundering and Counter-Terrorist Financing Rules

GENERAL PROVISIONS

PART 1

Article 1:

Preliminary

The objectives of these Rules

The objectives of these Rules are that all authorised and registered persons must comply fully with the controls and procedures issued by the Capital Market Authority to ensure that:

(a). fully apply the Anti-Money Laundering Law issued by Royal Decree No. M / 31 dated 11/05/1433H and its implementing Regulation, and apply the requirements of the FATF's 40 Recommendations and 9 Special Recommendations dealing with anti-money laundering and combating the financing of terrorism, the International Convention for Suppression and Financing of Terrorism (New York 1999), the United Nations Convention on Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna 1988) and the United Nations Convention (against transnational) on Organized Crime (Palermo 2000) and UN Security Council Resolutions 1267 and 1373 and successor resolutions related to combating terrorist financing.

(b). the credibility, integrity and reputation of the capital market is maintained.

(c). Authorised Persons and their clients are protected from illegal transactions involving money laundering, terrorist financing or other criminal activity.

Article 2:

Definitions

1- For the purpose of implementing these Rules, the following expressions and terms shall have the meaning they bear as follows unless the contrary intention appears:

Accounts are to be read to include any business relationships between Authorised Person and its client.

Beneficial owner – refers to the natural person(s) who ultimately own(s) or control(s) the funds of the clients or on whose behalf a transaction or activity is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

Business relationship - means professional or commercial relationship between an Authorised Person and a client. A relationship need not involve the Authorised Person

in an actual transaction; giving advice shall also constitute establishing a business relationship.

Client – refers to a customer, execution-only customer either natural or legal person and counterparty for whom an Authorised Person executes securities business.

Counterparty – a client who is an authorised person, an exempt person, an institution or a non-Saudi financial services firm**.**

FIU the Financial Intelligence Unit mentioned in the Anti-Money Laundering Law issued by Royal Decree No. M / 31 dated 11/5/1433H and its implementing Regulation.

Funds - means assets or properties of whatever value or type, material or non-material, tangible or intangible movable or immovable, along with documents of whatever type including electronic or digital systems, and bank documents that refer to an ownership or interest such as every type of checks, transfers, shares, securities, bonds, promissory notes, and guarantee letters.

Money Laundering refers to comitting or attempting to commit any act for the purpose of concealing or disguising the true origin of funds acquired by means contrary to *Shari'ah* or law, thus making the funds appear as if they had come from a legitimate source.

Non-profit Organizations refers to every legal entity engages in collecting, receiving, or paying money for charitable, religious, cultural, educational, social, or solidarity purposes or that conduct other charitable activities.

Politically Exposed Person (PEP) – PEPs are individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.

Terrorist financing – refers to the financing of terrorist acts, terrorists and terrorist organizations.

FATF - Financial Action Task Force on money laundering and terrorist financing**.**

Attachment shall mean the provisional ban on transferring, exchanging, disposing with or moving funds and proceeds or attaching same pursuant to an order by a court or a competent authority.

2- Without prejudice to paragraph (1) of this article, expressions and terms in these Rules have the meanings which they bear in the Capital Market Law and in the Glossary of defined terms used in the Regulations and Rules of the Capital Market Authority.

PART2

General application of AML/CFT requirements

Article 3:

General principles

1. Authorised Person must, in establishing policies and procedures to prevent money laundering and terrorist financing, consider carefully the specific nature of its business, organisational structure, type of client and transaction, and shall ensure that the measures taken by it are adequate and appropriate to meet the requirements and general objectives set out in these Rules.

2. Saudi Arabia has ratified and implemented the United Nations Convention on Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna 1988), the United Nations Convention on Organized Crime (Palermo 2000) and the International Convention for Suppression and Financing of Terrorism (New York 1999). These Conventions require to establish systems, controls and procedures aimed at preventing money laundering and terrorist financing, including procedures for reporting suspected money laundering or terrorist financing transactions. The board of directors and the general manager or the owner or the delegate of Authorised Person is responsible for establishing appropriate and effective policies and procedures for the prevention of money laundering and terrorist financing and to ensuring compliance with those policies and with all relevant legal and regulatory requirements. To ensure this, senior management must appoint a director or senior manager with direct responsibility for over-sighting compliance with the AML/CFT policies and procedures and relevant legal and regulatory requirements.

3. Authorised Person is required to:

   (a) issue an effective statement of policies and procedures aimed at preventing money laundering and terrorist financing, and ensuring compliance with current legal and regulatory requirements including the maintenance of records; and co-operation with the FIU and relevant law enforcement authorities in accordance with the relevant regulations and rules, including the timely disclosure of information;

   (b) ensure that the content of these Rules is understood by all officers and employees, and that they are aware of the requirements and vigilant in guarding against money laundering and terrorist financing;

   (c) regularly review the policies and procedures on prevention of money laundering and terrorist financing to ensure their effectiveness. For example, reviews performed by the internal audit or compliance officer to ensure compliance with policies, procedures and controls relating to prevention of money laundering and terrorist financing (areas of review shall include: (i) an assessment of the system for detecting suspected money laundering and terrorist financing transactions; (ii) evaluation and

checking of the adequacy of reports generated on large and / or irregular transactions; (iii) review of the quality of reporting of suspicious transactions; and (iv) an assessment of the level of awareness of front line staff regarding their responsibilities); and

(d) adopt client acceptance policies and procedures, and undertake required Customer Due Diligence ("CDD") measures, as set out in Part (3), including taking into account the risk of money laundering and terrorist financing depending on the type of client, business relationship or transaction.

Article 4:

Application of policies and procedures to overseas branches and subsidiaries

1. Authorised Person must ensure that its overseas branches and majority-owned subsidiaries ("subsidiaries") comply with the laws and regulations of Saudi Arabia concerning money laundering and terrorist financing, and the FATF Recommendations, to the extent that the laws and regulations applicable in the host country permit.

2. Authorised Person shall pay particular attention to the application of paragraph (1) of this article in its branches and subsidiaries which are located in countries that do not or insufficiently implement the FATF's Recommendations including jurisdictions designated as such by the FATF.

3. Where the minimum AML/CFT requirements of Saudi Arabia and host countries differ, branches and subsidiaries in host countries shall apply the higher standard, to the extent that host country laws and regulations permit. Where the law of the host country conflicts with Saudi Arabian law or regulations such that the overseas branch or subsidiary is unable to fully observe the higher standard, the Authorised Person's head office shall report this to the Authority and comply with such further directions as may be given by it.

4. Where an overseas branch or subsidiary is unable to observe group standards because this is prohibited by host country laws, regulations or other measures, the Authorised Person shall inform the Authority immediately.

Article 5:

Cash Payments

At no time, whether at the commencement of or during a business relationship shall an Authorised Person accept cash from a client, whether for investment purposes or as payment for services provided by the Authorised Person.

PART 3

CUSTOMER DUE DILIGENCE

Article 6:

For the purposes of these rules and before accepting any client, the authorised person must prepare a "Know Your Customer" form containing the information required by Annex (5-3) of the authorised persons regulations and the other information required by these rules.

Article 7:

Client Acceptance

1. Authorised Person must develop client acceptance policies and procedures that aim to identify the types of clients that are likely to pose a higher risk of money laundering and terrorist financing. A more extensive customer due diligence process must be adopted for higher risk clients, and this must include clear internal policies on the approval of a business relationship with such clients.

2. In determining whether a particular client or type of clients may be higher risk, Authorised Person must take into account factors such as the following:

   (a) the background or profile of the client;
   (b) the nature of the client's business, and the degree of money laundering or terrorist financing risk;
   (c) the place of establishment of the client's business and location of the counterparties with which the client does business, such as countries designated by the FATF or those known to the Authorised Person to lack proper standards in the prevention of money laundering or terrorist financing;
   (d) unduly complex structure of ownership for no good reason;
   (e) means of payment as well as type of payment (third party cheque the drawer of which has no apparent connection with the prospective client may be a cause for increased scrutiny);
   (f) any other information that may suggest that the client is of higher risk (e.g. knowledge that the client has been refused a business relationship by another financial institution).

3. Authorised Person must reconsider the risk categorization of a client if, following acceptance of the client, the pattern of account activity of the client does not fit in with the Authorised Person's knowledge of the client. Authorised Person must also consider making a Suspicious Transaction Report (STR).

4. Authorised Person must not accept any client or open an account for a client without meeting the client directly face-to-face, except where article (14) of these Rules applies.

Article 8

Customer Due Diligence (CDD) – general

1. Authorised Person must take all steps necessary to be able to establish the true and full identity of each client, and of each client's financial situation and investment objectives. Authorised Person must not open anonymous accounts, accounts using false or fictitious names, or accounts for prohibited persons notified by the Authority.

2. CDD must be carried out on all clients, and CDD requires Authorised Person to take the following steps:

   (a) Identify the client and verify their identity using the original documents prescribed in the AML Law and its implementing Regulation and paragraph (4) of this article. This also applies to all persons with signatory authority over the account;
   (b) identify and verify beneficial ownership and control using the original documents prescribed in the AML Law and its implementing Regulation and paragraph (4) of this article.
   (c) obtain information on the purpose and intended nature of the business relationship – depending on the type of client, business relationship or transaction, Authorised Person must obtain sufficient information such that ongoing due diligence on the client can be appropriately conducted; and
   (d) Ensure applying ongoing due diligence and scrutiny, i.e. perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the Authorised Person's knowledge of the client, the client's profile, taking into account, where necessary, the client's source of funds.

3. Authorised Person must apply the specific requirements CDD of Article (13) dealing with investment funds.

4. Authorised Person shall verify the identity of clients and any beneficial owners by checking the valid original documents as follows:

(a) Natural Persons:

- Saudi nationals:

- The client's National Identification Card or family record.
- The client's residential address & place of work and work address.

- Individual expatriates:

- A residence permits *(Iqamah)* or a five-year special residence permit or a passport, and a National Identification for Gulf Cooperation Council (GCC) nationals or a diplomatic identification card for diplomats.
- The client's residential address & place of work and work address.

(b) Legal persons:

For all clients that are legal persons, Authorised Person must obtain sufficient information about the nature of the business and its ownership and control structure so that it can identify the individual(s) that ultimately own(s) or control(s) the client. Specimen signatures shall be obtained for all account signatories.

- Companies:

- A copy of Commercial register issued by the competent authority.
- A copy of the Articles of association, or the memorandum of association and their annexes, and any amendments
- A copy of the identification card of the manager in charge.
- A copy of the issued resolution forming the Board of Directors.
- A copy of the Board resolution evidencing the approval of the opening of the account and conferring Authorization on the signatories;
- A List of the persons authorised who are qualified to deal with the accounts, pursuant to what is provided for in the commercial register, and a copy of the identification card of each.
- A List of all company's owners whose names are included in the memorandum of association and a copy of identification card of each.
- If the company has activities that require license from another government authority, a copy of that license is required.

- Non-profit Organizations:

- A copy of the license issued by the relevant government authority.
- A copy of the Board resolution evidencing the approval of the opening of the account.
- A copy of the articles of association.
- Authorization from the board of directors for the persons whom would open & deal with & operate the accounts and a copy of the identification card of each.
- A copy of the Authority's approval of accepting the client & open account for.

- Government entities:

- A copy of all required documents in accordance with its Law and organization regulatory.
- A copy of the authority approval of accepting the client & open account for.

(c) If a client is a type of legal person other than one of the types set out in paragraph (4/b) of this article, the Authorised Person must obtain the approval of the Authority.

5. For all clients, except where the Authorised Person is relying on a third party in accordance with Article (14) of these Rules, the identity of a prospective client shall be verified face to face at an Authorised Person before an account is opened or a business relationship is commenced.

6. If there is doubt or difficulty in determining whether the document obtained to verify identity is genuine, Authorised Persons must not open the account, and shall consider whether they need to make a suspicious transaction report.

7. Authorised Person must retain copies of all documents used to verify the identity of the client pursuant to Part (4) from these rules,

8. For the purpose of assisting an Authorised Person to identify the beneficial owner of an account, the Authorised Person must, when establishing a business relationship, ask whether the client is acting for his or its own account or for the account of another party or parties.

9. An Authorised Person must understand the purpose and intended nature of the business relationship or transaction, but additional information might also need to be obtained, and this could include some or all of the following information:

   - record of changes of address;
   - the expected source and origin of the funds to be used in the relationship;
   - initial and ongoing source(s) of wealth or income;
   - copies of the financial statements;
   - the various relationships between signatories with underlying beneficial owners;
   - The anticipated level and nature of the activity that is to be undertaken through the relationship.

Article 9:

Risk-based approach – reduced and enhanced costumer due diligence

1. All clients shall be subject to the full range of CDD measures on the basis of materiality and risk. The only exception to this rule is, that on the basis of the lower risk, and the fact that information on the identity of the client and beneficial owners is publicly available, Authorised Person may perform reduced CDD measures on a client that is a company listed on the stock exchange of a country sufficiently implement the FATF's Recommendations, or is a subsidiary of such a listed company. In such a case, only the requirements of article 8(2)(a),(c) and (d) need be carried out. However, where such a listed company is closely held i.e. subject to the beneficial ownership/control of an individual or a small group of individuals, an Authorised Person shall carefully review the AML/CFT risks and consider whether it is necessary to verify the identity of such individual(s).

2. Authorised Person must adopt an enhanced CDD process referred to Part 3 of these rules, for higher risk type of clients, business relationships or transactions. The relevant enhanced CDD process may vary from case to case depending on clients' background, transaction types and specific circumstances. Authorised Person must exercise its own judgment and adopt a flexible approach when applying the specific enhanced CDD measures to clients of particular high risk types.

3. Authorised Person must establish clearly in its client acceptance policies the risk factors for determining what types of clients and activities are to be considered as high risk, while recognising that no policy can be exhaustive in setting out all

risk factors that must be considered in every possible situation, such risk factors must include client risk, country, geographic risk and product/service risk.

4. In assessing whether or not a country sufficiently applies the FATF standards in combating money laundering and terrorist financing, Authorised Person must:

   (a) carry out an assessment of the standards of prevention of money laundering and terrorist financing. This could be based on Authorised Person's knowledge and experience of the country concerned or be acquired from relevant authority. The higher the risk, the greater the due diligence measures that must be applied when undertaking business with a client from the country concerned;
   (b) pay particular attention to assessments of compliance with the FATF Recommendations that have been undertaken by the FATF, FATF-style regional bodies, or the International Monetary Fund (IMF) and the World Bank; and
   (c) maintain an appropriate degree of ongoing vigilance concerning money laundering and terrorist financing risks and to take into account information that is available to Authorised Persons about the standards of AML/CFT systems and controls that operate in the country with which any of their clients are associated.

5. Apart from the risk factors set out in paragraph (3) of this article for determining a client's risk profile, the following are some examples of high risk types of clients:

   (a) complex legal arrangements that have no apparent legal or economic purpose;
   (b) persons (including companies and other financial institutions) from or in countries which do not or insufficiently apply the FATF's Recommendations e.g. countries designated as such by the FATF; and
   (c) PEPs.

6. Authorised persons must perform enhanced due diligence on higher risk clients. In higher risk cases. The Authorised Person must consider applying other additional measures such as:

   (a) Obtaining declarations in writing from the beneficial owners about the identity of, and the relationship with the directors and substantial shareholders;
   (b) obtaining comprehensive client profile information; e.g. extra information on the purpose and reasons for opening the account, business or employment background, source of funds and anticipated account activity;
   (c) assigning designated staff to serve the client and those staff must conduct CDD and more frequent ongoing monitoring, in order to ensure that any unusual or suspicious transactions are identified on a timely basis; and
   (d) Conducting face-to-face meetings with senior management of the client on a regular basis throughout the business relationship;
   (e) obtaining the approval of senior management of the Authorised Person when opening an account.

Article 10:

Politically exposed persons (PEP)

1. Authorised Person shall have risk management systems in place to identify whether a client or potential client, or a beneficial owner, is a PEP. Any accounts identified as being held by such persons shall be considered higher risk and Authorised Person shall conduct enhanced ongoing monitoring of such accounts.

2. The opening or continued operation of an account for a PEP must be approved by senior management of the Authorised Person pursuant to these article.

3. Where an authorised person has accepted a client and the client or the beneficial owner is subsequently found to be, or subsequently becomes a PEP, the authorised person shall obtain senior management approval to continue the business relationship.

4. Authorised Person shall take measures to establish the source of wealth and source of funds of PEPs that are clients or beneficial owners.

Article 11:

Non-profit Organizations

Authorised Person shall have in place policies, procedures and controls to comply with the Authority's requirements regarding the opening and handling of accounts and transactions for non-profit organizations. The following requirements shall be observed when dealing with accounts of any such organizations:

(1) Non-profit organizations must have an official registration/license issued by the relevant government authority, specifying the purposes and activities of the organization.
(2) Authorised Person shall classify non-profit organizations as high risk, and shall apply enhanced due diligence when dealing with such clients.

Article 12:

When Authorised Person must perform CDD

1. An Authorised Person must carry out CDD measures when it:

   (a) opens an account or establishes a business relationship;
   (b) suspects money laundering or terrorist financing; or
   (c) doubts the veracity of documents, data or information previously obtained for the purpose of identification or verification.

2. In general, an Authorised Person must verify the identity of the client or potential client and beneficial owner before or during the course of establishing the business relationship. When the Authorised Person is unable to perform the CDD process satisfactorily at the account opening stage, it must terminate the

business relationship and not perform any transaction, and must consider whether a Suspicious Transaction Report (STR) must be made.

Article 13:

Investment Funds

1. Where Authorised Person act for a client who is investing in an investment fund or a real estate investment fund, Authorised Person must carry out CDD on the client and shall comply with the other requirements of these Rules, except that where the client is a counterparty, the Authorised Person need not identify and verify the identity of the beneficial owners that are investing through the counterparty, provided that the requirements of paragraph (2) of this article are met.

3. The Authorised Person must ensure that the counterparty:

(a) is regulated, and licensed by the relevant government authority;
(b) is based in a jurisdiction that adequately applies the FATF Recommendations;
(c) is applying, as a minimum, requirements for AML/CFT (including measures for CDD and identification of beneficial owners) that are consistent with the requirements of these Rules and of the FATF Recommendations and
(d) has entered into an agreement with the Authorised Person agreeing, that upon the request of the Authorised Person or the Authority, the counterparty will provide any information requested regarding the beneficial owners.

Article 14:

Reliance on other third parties for CDD

1. This Article refers to a third party that introduces clients to an Authorised Person and performs the client identification and verification. For the purposes of this article, a third party must either be a commercial bank or financial institution that engages in securities activities.

2. The Authorised Person may rely on the third party to perform elements in subparagraph (a) to (c) of the CDD measures in paragraph (2) article (8) of these Rules provided that the criteria set out below are met. However, the ultimate responsibility of client identification and verification always remains with the Authorised Person and not with the third party.

3. Authorised Person can only rely on third parties to perform the CDD if the client is located in a country other than Saudi Arabia.;

4. Prior to reliance, Authorised Person must satisfy itself that it is reasonable to rely on a third party to apply the CDD and that the CDD measures are as rigorous as those which the Authorised Person would have conducted itself for the client. Authorised Persons must establish clear policies in order to

determine whether the third party in question possesses an acceptable level of reliability.

5. Authorised Person relying upon a third party must:

(a) obtain copies of the CDD documentation and information, as required by paragraphs (2/a) to (2/c) of Article (8) of these Rules, including other information referred in article (6) of these rules;
(b) take adequate steps to satisfy itself that copies of relevant documentation relating to the CDD requirements will be made available from the third party upon request immediately, such as establishing their respective responsibilities in writing, including reaching an agreement with the third party that copies of other relevant documentation relating to the CDD requirements will be made available from the third party upon request immediately and the Authorised Person will be permitted to verify the CDD undertaken by the third party at any stage; and
(c) ensure the third party is regulated and supervised by a competent authority, and has measures in place to comply with CDD and record keeping requirements in line with these rules and the FATF recommendations.

6. Authorised persons must conduct periodic reviews to ensure that a third party upon which it relies, continues to conform to the criteria set out above. This may involve review of the relevant policies and procedures and sample checks of the due diligence conducted.

7. Authorised persons must not rely on third parties based in country considered as high risk, such as countries that have no or inadequate AML/CFT systems.

Article 15:

Acquisition

When an Authorised Person acquires, either in whole or in part, a financial institution in a foreign country, the Authorised Person shall ensure that the acquired financial institution has or will perform CDD measures consistent with the requirements in these Rules at the time of acquisition unless:

(a) the subsidiary it acquired holds the CDD records for all clients (including all relevant client identification information) and the Authorised Person has no doubt or concerns about the veracity or adequacy of the information so acquired, and

(b) the Authorised Person has conducted due diligence enquiries that have not raised any doubt on its part of as to the adequacy of AML/CFT procedures and controls previously adopted by the other financial institution.

Article 16:

Non-face to face business relationships

1. An Authorised Person shall consider money laundering and terrorist financing threats that may arise from the misuse of new or developing technologies, and must formulate its policies, procedures and controls, to prevent such threats.

2. An Authorised Person must formulate its policies, procedures and controls in a way that addresses the specific risks associated with non-face to face business relationships and transactions. The specific risks associated with non-face to face business relationships must be addressed by specific and effective measures, both at the time the business relationship is established and as part of ongoing CDD.

Article 17:

Ongoing CDD and Unusual Transactions

1. An Authorised Person must monitor on an ongoing basis the business relationships it has with clients. It must during the course of such relationships, monitor the conduct of the client's account and scrutinise transactions undertaken to ensure that the transactions are consistent with the Authorised Person's knowledge of the client, its business and risk profile and the source of funds.

2. Authorised Person must pay attention to all complex, large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose.

3. Authorised Person shall pay special attention to business relationships and transactions with clients or financial institutions from countries which do not or insufficiently apply the FATF's Recommendations. Where the Authority advises Authorised Person that such countries continue to not or insufficiently apply the FATF's Recommendations, Authorised Person shall treat all business relationships and transactions as higher risk and shall apply the measures set out in paragraph (6) of article (9) of these Rules.

4. The background and purpose of all such transactions, including transactions that have no economic or visible legal purpose, must be examined, the findings established in writing and those findings must be retained for at least 10 years and be made available to the Authority, and internal and external auditors if requested.

Article 18:

Review and updating of records

Identification data collected under the CDD process must be kept up-to-date, accurate and relevant. Authorised Person must undertake annual or ad hoc reviews of existing records, particularly for higher risk categories of clients or business relationships, when appropriate trigger events occur. Examples of trigger events that might prompt an Authorised Person to seek appropriate updated information include:

- an existing client applying to open a new account or establish a new relationship, or significantly alter the nature of an existing relationship;
- when there is a transaction that is unusual or not in line with the client's normal trading pattern based on the Authorised Person's knowledge of the client; or
- when the Authorised Person is not satisfied that it has sufficient information about the client or has doubts about the veracity or adequacy of previously obtained identification data.

PART 4

Record Keeping

Article 19:

Record Keeping Requirements

1. Authorised Person shall ensure to comply with the record keeping requirements contained in the relevant rules & regulations of the Authority and the company Saudi Stock Exchange (Tadawul), and must keep a record of all client identification data and other information and documents obtained as part of the CDD process, account files and business correspondence, as well as all transaction records.

2. Authorised Person shall maintain sufficient records to permit reconstruction of individual transactions (including the amounts and types of currencies involved) so as to provide, if necessary, evidence for prosecution of criminal activity.

3. Authorised Person shall keep the type of information regarding the accounts of its clients in particular the following:

   (a) details of the client and beneficial owner(s) (if any) of the account, and any other CDD information required;
   (b) account details, including the volume of the funds flowing through the account; and
   (c) for transactions: the origin of the funds, the form in which the funds were provided or withdrawn, such as, cheques, transfer, the identity of the person undertaking the transaction, the destination of the funds, and the form of instruction and authorization.

4. Authorised Person shall ensure that all client and transaction records and information are available on a timely basis to the Authority.

5. All records on transactions, both domestic and international, shall be maintained by Authorised Person for at least ten years after the date of the transaction.

6. All CDD records, account files and business correspondence shall be kept by Authorised Person for at least ten years after the account is closed.

7. In situations where the records relate to on-going investigations or where records relate to transactions which have been the subject of a suspicious transaction report, they shall be retained until it is confirmed that the case has been closed even if this is still ongoing after 10 years.

8. Authorised Person may retain documents as originals or copies, in paper or electronic form, provided that they are admissible as evidence in a court of law.

PART 5

Suspicious Transaction Report

Article 20:

Suspicious Transaction Report

1. Consistent with the obligations set out in the AML Law and its implementing Regulations, Authorised Person must immediately report to the FIU any complex, huge or unusual transaction or raises doubt and suspicion concerning its nature and purpose, or is related to money laundering, financing of terrorism, terrorist acts, or terrorist organizations.

2. Within 10 days the Authorised Person must submit a detailed report setting out all available data and information about the suspicious transactions and parties involved to the FIU. At a minimum the report shall include the following details:

    - Account statements for a period of six (6) months
    - Copies of all account opening documents
    - Any data related to the nature of the reported transactions
    - The indications and justifications for the suspicion, along with all supporting documents

3. Suspicious transactions must be reported regardless of whether they are also thought to involve other matters. The fact that a report may have already been filed with the FIU in relation to previous transactions of the client in question must not necessarily preclude the making of a fresh report (without delay) if new suspicions are aroused.

4. Authorised Person shall appoint an appropriately senior employee within the Authorised Person to whom all staff are instructed to promptly refer all complex, huge or unusual transaction or raises doubt and suspicion concerning its nature and purpose, or is related to money laundering, financing of terrorism, terrorist acts, or terrorist organizations, for possible referral to the FIU as an STR. The senior officer (referred hereafter as the Money Laundering and Terrorism Financing Reporting Officer (MLRO)). must be a registered person, and have sufficient academic, scientific and practical experience in AML/CFT.

5. The MLRO shall act as a central reference point within the Authorised Person to facilitate onward reporting to the FIU. The MLRO must play an active role in the identification and reporting of suspicious transactions, and shall review reports of large or irregular transactions generated by the Authorised Person's internal systems on a regular basis as well as of ad hoc reports made by any employee of the Authorised Person.

6. Where Authorised Person employee brings a transaction to the attention of the MLRO, the circumstances of the case shall be reviewed at that level to determine whether the suspicion is justified. If a decision is made to not report the

transaction to the FIU, the reasons for this shall be fully documented by the MLRO.

7. Authorised Person must keep records of all transactions referred to the MLRO, together with all internal findings and analysis done in relation to them. A register must be maintained of all STR made to the FIU as well as of all reports made by employees to the MLRO, including those where a decision is made by the MLRO not to report to the FIU.

8. Authorised Person shall use the standard form prescribed by the FIU for reporting, and must report by fax, email or any other means agreed by the FIU to ensure that the FIU receives the report promptly. If reports are initially made by telephone, the STR must be confirmed in writing within 24 hours.

9. The Authorised Person must verify that it has received an acknowledgement of receipt from The FIU.

10. Authorised Person must continue to monitor the account and the client, and must send a further STR if appropriate in the case where a response is not received from the FIU regarding an STR

11. A list of indicators of types of potentially unusual or suspicious transactions or activities that could be a cause for further scrutiny is set out in Annex 1 of these Rules. The list is not exhaustive and Authorised Person must remain vigilant to their obligation to report any unusual or suspicious transactions or activity, whether these are of a type set out in Annex 1 of these Rules or not. The existence of one or more of the factors described in the list warrants some form of increased scrutiny of the transaction, but by itself does not necessarily mean that a transaction is suspicious.

12. In relation to terrorist financing, the FATF issued a paper in April 2002 on guidance for financial institutions in detecting terrorist financing, and a further report on terrorist financing typologies in March 2008. Authorised persons shall ensure that their staff are familiar with these documents.

13. Where the FIU requires further information from an Authorised Person to follow up on an STR, the Authority will act as a conduit for the request and shall ask the Authorised Person to provide the information requested by the FIU.

14. In accordance with the AML Law article 28 authorized persons and their directors, officers and employees (permanent and temporary) are protected by law from both criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report unusual or suspicious transactions or activity in good faith to the FIU. This protection is available even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

Article 21:

Tipping Off

1. In all circumstances, Authorised Person, its directors, officers and employees must ensure that clients or related parties are not alerted to the fact that they have made or are considering making an STR or providing documents or information linked to an STR to the FIU. An Authorised Person shall at all times keep its reporting of suspicious transactions highly confidential, and reports of suspicious transactions or reports that are to be reviewed by the MLRO for possible reporting shall be accessible only by specifically authorised staff of the Authorised Person.

2. Where an STR has been made to the FIU and it becomes necessary to make further enquiries of the client, great care must be taken to ensure that the client does not become aware that the STR has been made. The Authorised Person shall continue its business dealing with the reported clients as usual, it must not warn its clients or other relevant parties of the suspicious transactions, and it shall await further instructions from the Authority.

Article 22:

Designated persons – UNSCR Resolutions)

1. Authorised Person must have in place effective procedures to promptly identify any clients or potential clients (including beneficial owners) that have been designated ("designated persons") by the United Nations Committee under UNSCR 1267(1999) ("the 1267 Committee"); and successor resolutions.

2. If an Authorised Person identifies a client or potential client as a designated person or a transaction where one of its parties is a designated persons, it must immediately send an STR to the FIU and a copy of the STR to the Authority, and must immediately freeze any property that it holds for a designated person. Once an STR is made, the Authorised Person shall continue freezing the account and transactions of the client until receive instructions from the Authority.

3 Prior to opening any new account, Authorised Person must check the potential client's name against the lists of designated persons. Authorised persons must, on a daily basis, check the names of all existing clients against the lists of names of designated persons by reviewing the UN website.

4. Where a person is listed by the competent authority in Saudi Arabia under UNSCR 1373 (or a successor resolution), the Authority will notify all Authorised Persons of that listing and they must immediately freeze the property of such persons.

5. Where funds that have been frozen, are unfrozen because the designated person has been delisted, or because the person whose assets were frozen was incorrectly thought to be a designated person, or because authorisation was

made by the competent authority to release funds for legal or living expenses, then the Authority will notify the Authorised Person.

PART 6

Internal policies, procedures and controls

Article 23:

Internal Policies and Compliance

1. Authorised Person shall develop and implement internal policies, procedures and controls to help prevent money laundering and terrorist financing and must communicate these to its employees. The compliance officer shall also ensure compliance with the AML/CFT policies, procedures and controls.

2. The policies, procedures and controls must include, amongst other things, CDD measures, record retention, the detection of unusual and/or suspicious transactions and the obligation to make an STR.

3. An Authorised Person shall ensure that the MLRO and any of its staff (performing compliance function) have timely access to all client and transaction records and other relevant information which they require to discharge their functions.

4. The MLRO shall undertake the following duties:

    - Develop, update and implement the Authorised Person's system, procedures and controls on AML/CFT.
    - Keep pace with developments in AML/CFT laws and regulations, trends, techniques, and update indicators of money laundering or terrorist financing.
    - Ensure that the Authorised Person complies with its policies and procedures**.**
    - Receiving directly from staff any reports of suspicious transactions or activity And analyse those reports and then decide whether to file an STR with the FIU.
    - Prepare a report annually to the Board of the Authorised Person setting out all actions that have been taken to implement the internal policies, procedures and controls and proposals for increasing the effectiveness and efficiency of the procedures. Thereafter, the report shall be submitted to the Authority.
    - Ensure that staff of the Authorised Person maintains all necessary records.
    - Organise ongoing training for all staff of the Authorised Person.

Article 24:

Internal Audit

1. The internal audit in the Authorised Person shall regularly assess the effectiveness of the Authorised Person's internal AML/CFT policies, procedures and controls and the Authorised Person's compliance with these Rules.

Article 25:

Education and Training

1. Authorised Person must take all appropriate steps to ensure that their staffs (group-wide) receive regular training on:

   (a) AML/CFT agreements, laws and instructions, and in particular, CDD measures, detecting and reporting of suspicious transactions;
   (b) prevailing techniques, methods and trends in money laundering and terrorist financing; and
   (c) the Authorised Person's internal policies, procedures and controls on AML/CFT and the roles and responsibilities of staff in combating money laundering and terrorist financing.

2. Authorised persons must have educational programmes in place for training all new employees. Refresher training must also be provided at regular intervals to ensure that staff, in particular those who deal with the public directly and help clients open new accounts.

PART 7

Closing Provisions

Article 26:

Sanctions

Without prejudice to the sanctions imposed under AML Law, Authorised Person or any director, manager or employee of an Authorised Person that fails to comply with any article of these Rules shall be subject to the sanctions set out in Articles 59 and 62 of the Capital Market Law.

Article 27:

Publication and Entry into Force

These Rules shall become effective upon their publication.

Annex 1

Securities Business Indicators for Money Laundering or Terrorist Financing

Examples of possible indicators that a transaction or activity may be linked to money laundering or terrorist financing are as follows:

1. The client exhibits unusual concern regarding the firm's compliance with AML/CFT requirements, particularly with respect to his identity and type of business.

2. Client refuses to identify himself or to indicate legitimate sources for his funds and other assets.

3. The client wishes to engage in transactions that have no apparent legal or economic purpose or are inconsistent with the declared investment strategy.

4. The client tries to provide the Authorised Person with incorrect or misleading information regarding his identity and/or source of funds.

5. The Authorised Person knows that the client was involved in money laundering or terrorist financing activities, or in other criminal offences or regulatory violations.

6. The client exhibits a lack of concern regarding risks, commissions, or other transaction costs.

7. An Authorised Person suspects that the client appears to be acting as an agent on behalf of an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information about that person or entity.

8. The client has difficulty describing the nature of his business or lacks general knowledge of his activities.

9. The client holds multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers with no apparent reason for that activity.

10. The client makes multiple of wire transfers to his investment account followed by an immediate request that the money be wired out to a third party without any apparent business purpose.

11. The client makes a long-term investment followed shortly thereafter by a request to liquidate the position and transfers the proceeds out of the account.

12. The client's activities vary substantially from normal practices.

13. A client refuses to provide the Authorised Person with basic information for a mutual fund to verify the client's identity.

14. The client requests that the Authorised Person uses wire transfers in such a manner that originator information is not transferred from the sending to the receiving destination.

15. A client seeks to change or cancel a transaction after being informed of the information verification or record keeping requirements by the Authorized Person.

16. The client requests that a transaction be processed in such a manner to avoid more documentation.

17. The client's account shows an unexplained high level of wire transfers with very low levels of securities transactions.

18. The Authorised Person knows that funds or property is proceeds that come from illegal sources.

19. Change source of funds constantly

20. The non-matching between the value or repetition of the operations with the information available on the suspect, his activity, income, lifestyle and attitude.

21. The beneficial owner belongs to an organization known of criminal activity.

22. The appearance of signs of luxury on the suspect and his family in an exaggerated way which might not match his economic status (especially if it was sudden).