



Resolution No. (53) of 2015
Regarding Issuance of CMA Regulations No. (2) of 2015
on AML/CFT

Having Perused:

- Law No. (7) of 2010 Regarding the Establishment of the Capital Markets Authority and Regulating Securities Activities and its Executive Bylaws, as amended; and
- CMA Regulations on Combating Money Laundering and Terrorist Financing No. (C .M .A. /S .S. /I.C/4/2013) issued on 17/7/2013;

And Based on CMA Board of Commissioners Resolution passed in its meeting No. (24) of 2015 held on 14/7/2015 on the approval of the amendments of CMA Regulations on Combating Money Laundering and Terrorist Financing No. (C .M .A. /S .S. /I.C/4/2013) issued on 17/7/2013 for Licensed Persons.

The Following Was Resolved

Article (1): CMA Regulations No. (2) on Anti-Money Laundering & Combating the Financing of Terrorism ("AML/CFT") for Licensed Persons are hereby issued.

Article (2): Regulations on Combating Money Laundering and Terrorist Financing No. (C .M .A. /S .S. /I.C/4/2013) issued on 17/7/2013 are hereby cancelled.

Article (3): CMA Regulations No. (2) of 2015 on AML/CFT shall come into force from the issue date of these Regulations. These Regulations shall be enforced on all licensed persons.

Dr. Nayef Falah Al-Hajraf

Issued on 23/ 7 / 2015

**CMA Regulations No. (2) of 2015
on AML/CFT**

TABLE OF CONTENTS

Clause	Title	Page
	Preamble	5
First	Definitions	5
Second	General Principles	7
Third	Application of policies and procedures to overseas branches and subsidiaries of the Licensed Person	11
Fourth	Cash Payments	12
Fifth	Customer Acceptance	13
Sixth	Customer Acceptance Considerations	13
Seventh	General Provisions on CDD procedures	13
Eighth	Risk-based approach (Reduced or enhanced customer due diligence)	17
Ninth	Politically Exposed Persons (PEPs)	19
Tenth	Non-profit Organizations or Entities	20
Eleventh	Cases where the Licensed Person must Perform CDD	20
Twelfth	Collective Investment Schemes	21
Thirteenth	Reliance on third parties for CDD	21
Fourteenth	Acquisition	23
Fifteenth	Non-face-to-face business relationships	23
Sixteenth	Ongoing CDD and unusual transactions	24
Seventeenth	Review and updating of records	24
Eighteenth	Record keeping requirements	25
Nineteenth	Suspicious Transaction Report	26
Twentieth	Tipping Off	28
Twenty-first	Designated Persons on the United Nations Terrorist List	29
Twenty-second	Internal Policies and Compliance	29
Twenty-third	Audits	30
Twenty-fourth	Training	31
Twenty-fifth	Sanctions	32
Twenty-sixth	Publication and Entry into Force	32

CMA Regulations No. (2) of 2015 **on AML/CFT**

Preamble:

Pursuant to Law No. (7) of 2010 on the Establishment of the Capital Markets Authority and Regulating Securities Activities, to the AML/CFT Executive Regulation, the Anti-Money Laundering and Combating The Financing of Terrorism Law No. (106) of 2013, and to relevant UN resolutions.

These Regulations aim to ensure the compliance of the licensed persons with the procedures and controls thereof and achieve the following:

- a- Enhance the integrity and credibility of the financial market
- b- Protect the licensed persons and their customers from illegal transactions that may involve money laundering and financing of terrorism or any other criminal activity.

First: Definitions

The definitions set forth in Law No. (7) of 2010 on the Establishment of the Capital Markets Authority and its Executive Bylaws and the definitions of Law No. (106) of 2013 on Anti-Money Laundering and Combating the Financing of Terrorism and its Executive Regulation apply to these Regulations. In addition, the following words and expressions, wherever mentioned in these Regulations, shall have the meaning assigned to them unless specified otherwise in the text:

The Authority	Capital Market Authority
AML/CFT Law	Anti-Money Laundering and Combating the Financing of Terrorism Law No. (106) of 2013 and its Executive Regulation
Licensed Person	All persons covered under law No.(7) of the year 2010 concerning the Establishment of the Capital Markets Authority
The Unit	Kuwait Financial Intelligence Unit
Counterparty	A licensed person, non-Kuwaiti investment company or financial services facility
Non-profit Associations and Entities	A legal person (association or entity) that primarily engages in raising or disbursing funds for charitable purposes
Compliance Officer	Employee appointed as a compliance controller at the senior management level to be responsible for the implementation of the requirements of the AML/CFT Law, the CMA related regulations and other relevant legal and supervisory requirement.
Suspicious Transaction Report (STR)	A report filed by a licensed person with the KFIU pursuant to section 3 of the AML/CFT Law.
FATF	Financial Action Task Force on money laundering and terrorism financing.
Provisional Seizure	Temporary prohibition of transfer, remittance, exchange or disposal of funds, or provisional seizure thereof pursuant to an order from court or a competent authority.

Second: General Principles

- 1- A licensed person must consider the nature of its business, organizational structure, type of customers and transactions in establishing AML/CFT policies and procedures, and shall ensure that the measures taken by it are adequate and appropriate to meet the requirements and general objectives provided for in these Regulations.
- 2- The FATF recommendations on anti- money laundering and terrorism financing require setting out and implementing AML/CFT procedures. In line with such resolutions, licensed persons must establish systems, policies and procedures aimed at preventing money laundering and terrorism financing. The senior management of the licensed person is responsible for effectively managing the risks facing the business, including the risks of money laundering and financing of terrorism emanating from customers, geographic location and delivery channels. It must commit to setting adequate and effective policies and procedures to prevent money laundering and financing of terrorism, and to ensuring implementation and compliance with those policies and with all relevant regulatory and legal requirements. To ensure this, a compliance officer should be appointed at the senior management level with direct responsibility for overseeing compliance with AML/CFT policies and procedures, as well as other relevant legal requirements as set out in these Regulations and the AML/CFT Law. He is responsible for reporting to the Unit any suspected money laundering or terrorism financing in accordance with these Regulations.
- 3- The Licensed Person is required to:
 - a- Issue an effective statement of policies and procedures aimed at preventing money laundering and terrorism financing and, ensuring full compliance with all regulatory legal requirements, such as the maintenance of records and cooperation with the supervisory authorities responsible for compliance with the AML/CFT Law and relevant resolutions, and submit those policies to the

CMA through the Anti-Money Laundering Unit at the Authority, including the timely disclosure of information.

- b- Ensure that all officers, employees – and those who work for it (as consultants) – fully understand the content of these Regulations, are aware of the requirements and take all precautions to prevent money laundering and terrorism financing.
- c- Regularly review the policies and procedures on preventing money laundering and financing of terrorism to ensure their effectiveness, such as reviewing policies and procedures issued by the Internal Audit Unit or compliance officer to ensure compliance with them. This review covers the following areas:
 1. Assessment of the system for detecting money laundering and terrorism financing transactions.
 2. Evaluation and checking of reports on large or unusual transactions and verify their adequacy.
 3. Review of the quality of reporting of suspicious transactions.
 4. Assessment of the level of awareness of customer service employees regarding their responsibilities.
- d- Apply customer acceptance policies and procedures and undertake CDD measures as set out in Sections Fifth, Sixth, Seventh and Eighth of these Regulations, including taking into consideration risk of money laundering and terrorism financing depending on the type of customer, transactions and business relationship, geographic locations and products and delivery channels.
- e- Assess their risk of money laundering and terrorism financing, including risks of new products and technologies. The risk assessment and any underlying information shall be documented in writing, kept up-to-date and readily available for the CMA upon request.

- f- Put in place processes to identify, monitor, manage and mitigate money laundering and terrorism financing risks, giving consideration to:
1. Customer risk;
 2. Risks related to countries or geographic areas in which customers operate or the place of origination or destination of transactions;
 3. Risks related to the nature of products and services offered; and
 4. Risks related to the delivery channels for products and services.

Higher risk factors where Licensed Persons should apply enhanced CDD measures must be identified and include for instance the following:

1. Customer risk factors:
 - The customer's profile and background.
 - The nature of the customer's business and degree of money laundering and terrorism financing risk.
 - A business relationship conducted in unusual circumstances.
 - Non-resident customers.
 - Legal persons or arrangements that manage the assets of third parties.
 - Companies that have nominee shareholders or shares in bearer form.
 - Activities which are cash-intensive or susceptible to money laundering or terrorism financing.
 - The ownership structure of the company that appears unusual or excessively complex with no visible economic or lawful purpose given the nature of the company's business.
 - Business relationships and transactions conducted other than "face to face".
 - Business relationships conducted in or with countries as identified in item (2) below.

- High-risk Politically Exposed Persons ("PEPs") or customers linked to a PEP.
- High net worth customers, or customers whose source of income or assets is unclear.
- Means and type of payment. In this case, the Licensed Person must strictly verify whether the amount given by the customer to be deposited in his account is drawn on another person with no apparent connection with the customer.

2. Country or geographic risk factors:

- Countries classified by credible sources, such as mutual evaluation reports or published follow-up reports, as not having adequate AML/CFT systems.
- Countries identified by the Kuwait Financial Intelligence Unit as high risk.
- Countries subject to sanctions, embargos or similar measures issued by the United Nations for example.
- Countries classified by credible sources as having significant levels of corruption or other criminal activity.
- Countries or geographic areas classified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their territories.
- Place of establishment of the customer's business and location of the Counterparties (correspondent party) which the customer does business with, especially if the place of establishment or the location is in a country designated by the FATF or a country known to the Licensed Person as not applying adequate and sufficient AML/CFT standards.

3. Product, service, transaction or delivery channel risk factors:
 - Anonymous transactions (which may include cash).
 - Business relationships or transactions conducted with customers that are not physically present for the purpose of identification.
 - Payment received from unknown or un-associated third parties.

- g- Licensed Person shall adopt the following measures to mitigate the money laundering and terrorism financing risks:
 1. Assessing the various risk factors;
 2. Obtaining additional information on the customer, beneficial owner, beneficiary and transaction;
 3. Establishing a risk profile on customers and transactions
 4. Applying enhanced customer due diligence to high risk customers;
 5. Updating more regularly the information on all customers;
 6. Adopting other measures as may be prescribed by the CMA or the Kuwait Financial Intelligence Unit.

- h- Develop mechanisms to exchange available information and protect confidentiality of information with financial institutions, domestic and foreign branches and subsidiaries.

Third: Application of policies and procedures to overseas branches and subsidiaries of the Licensed Person

- 1- The Licensed Person must ensure that overseas branches and subsidiaries comply with the laws, regulations, and resolutions issued in Kuwait as well as the Licensed Persons internal policies, programs and procedures concerning anti- money laundering and combating terrorism financing, and with the FATF

recommendations to the extent permitted by the laws and regulations in the host country.

- 2- The Licensed Person must pay special attention to the application of paragraph (1) of Section Third in its branches and subsidiaries located in countries which do not or insufficiently apply the FATF recommendations, including countries designated as such by the FATF.
- 3- Where AML/CFT requirements of Kuwait and host countries differ, the Licensed Person must apply the best requirements on its branches and subsidiaries to the extent permitted by the laws and regulations of the host country.
- 4- Where an overseas branch or subsidiary fails to meet any of the AML/CFT requirements applicable in Kuwait because the laws and regulations of the host country do not permit that or for any other reason, it shall inform the CMA immediately and comply with any guidelines issued in this regard.

Fourth: Cash Payments

At no time, whether at the beginning or during a business relationship, shall a Licensed Person accept cash from a customer, whether for investment purposes or as payments for services provided by the Licensed Person.

With the exemption of Trivial service fees provided by the licensed persons, such as: Account opening fees, fees for printing different types of documents and certificates, and any other services provide by the licensed persons based on the following determinants:

- a- Payments should be paid by the customer or his legal representative.
- b- Payment amounts for the services should not exceed KD 100.
- c- Fees should be non-refundable.
- d- Due service fees should be paid in the form of one payment and not be broken down into small payments,
- e- Customer Due Diligence (CDD) should be applied, with the consideration of reporting any suspicious cases.

Fifth: Customer Acceptance

For the purposes of implementing the provisions of these Regulations, a Licensed Person should, prior to accepting any customer, prepare a “Know Your Customer” form containing the minimum information required by Sections Sixth and Seventh of these Regulations.

Sixth: Customer Acceptance Considerations

- 1- A Licensed Person must have in place customer acceptance policies and procedures to determine the type of customers that are likely to pose a higher risk of money laundering and terrorism financing. It must adopt extensive and detailed CDD policies and procedures for high-risk customers, such as clear internal policies on the approval of a business relationship with such customers. This shall also apply to PEPs where additional CDD measures should be put in place.
- 2- The Licensed Person must reconsider the risk assessment of a customer if the pattern of his account activity following acceptance does not fit in with the Licensed Person’s knowledge of the customer, and must also consider making a suspicious transaction report.
- 3- Except where Sections Thirteenth and Fifteenth of these Regulations apply, a Licensed Person must not accept any customer or open an account for a customer without meeting the client face-to-face.

Seventh: General Provisions on CDD procedures

- 1- The Licensed Person must take all steps necessary to obtain valid and full data on the customer, his financial situation and investment objectives. In all cases, anonymous accounts, accounts using false or fictitious names, or accounts for prohibited persons notified by the Authority must not be opened or maintained.
- 2- CDD measures must be carried out on all customers, which require the Licensed person to take the following steps:

- a- Identify and verify the identity of the customer using the original documents prescribed in paragraph (4) of this Section. This shall also apply to all persons with signatory authority over the account.
 - b- Understand the ownership and control structure of the customer.
 - c- Identify and verify the identity of the beneficial owners of the account and people who control it using original documents.
 - d- Obtain information on the purpose and nature of the business relationship depending on the type of customer, business relationship or transaction in order to apply ongoing CDD.
 - e- Ensure applying ongoing CDD, i.e. perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that all transactions are consistent with the Licensed Person's knowledge of the customer, the customer's profile, source of wealth and funds.
- 3- The Licensed Person must apply the specific CDD requirements of Section Twelfth of these Regulations about collective investment schemes.
- 4- When verifying the identity of the customer or beneficial owner, the Licensed Person must check the valid and official original documents as follows:
- a- Civil card for citizens and residents;
 - b- Passport or travel document for persons not residing in the state of Kuwait;
 - c- Commercial license issued by the Ministry of Commerce and Industry for resident companies and establishments and, in the case of non-resident companies and establishments documents issued by competent authorities in the state in which they were incorporated or established;
 - d- Documents, papers, instruments, and court orders proving that a person has been appointed to represent the concerned person;

- e- For customers not mentioned above, approved official identification documents attested by competent official authorities or bodies that issue these documents.
-
- 5- The Licensed Person must meet the customer, potential customer or beneficial owner face-to-face when verifying his identity prior to opening the account or engaging in a business relationship with him. If the customer fails to show up in person, the following steps shall be taken:
 - a- Authenticate the documents in accordance with relevant laws and procedures,
 - b- Request additional documents and establish separate procedures to verify the identity of the customer and/or contact him.
 - 6- If there is doubt or difficulty in determining whether the document presented by the customer to verify his identity is genuine, the Licensed Person must not open the account and shall consider the need to make a suspicious transaction report.
 - 7- The Licensed Person must retain copies of all documents used to verify the identity of the customer pursuant to the provisions of Section Eighteenth of these Regulations.
 - 8- For the purpose of assisting a Licensed Person to identify the beneficial owner of an account, the Licensed Person must, when establishing a business relationship, ask whether the customer is acting for his own account or for the account of another party or parties. For this instance, the Licensed Person must obtain a paper signed by the customer upon establishing the relationship certifying that the customer is the beneficial owner of the account, or request other types of documents that the Licensed Person deems necessary.
 - 9- The Licensed Person must understand the purpose and intended nature of the business relationship or transaction. Additional information on the customer might also be needed, including some or all of the following information:
 - a- Record of changes of address,

- b- Copies of the financial statements,
- c- Any relationship between the beneficial owners and signatories,
- d- The nature and anticipated level of the activity to be undertaken through this relationship with the customer.

10- Where a Licensed Person is undertaking a transaction with a firm licensed outside Kuwait through an omnibus account or for named customers through a designated account, the Licensed Person must compel the licensed firm to provide a written assurance that the identity of all the underlying customers has been verified in accordance with its local requirements. These requirements must be in line with those applicable in Kuwait. Where such an assurance cannot be obtained, the transaction should not be undertaken.

Furthermore, the Licensed Person should implement the aforementioned CDD measures with respect to the following:

- a- Before or during the course of establishing a business relationship with a customer;
- b- Before carrying out a transaction above the limit set forth in the Executive Regulation of the AML/CFT Law for a customer with whom the Licensed Person is not in an established business relationship, whether it is conducted as a single transaction or several transactions that appear to be linked;
- c- Before carrying out a domestic or international electronic transfer for the customer;
- d- Whenever there is a suspicion of money laundering or terrorism financing;
- e- Whenever there are doubts about the veracity or adequacy of previously obtained customer identification data.

11- In the cases where the Licensed Person deal with foreign customer through "Global Custodian" a written certificate should be obtained from the global

custodian proofing his full abidance to all FAFT recommendations specially customer due diligence. In addition, the Licensed Person has to acquire the minimum information required from the customer.

Eighth: Risk-based approach (Reduced or enhanced customer due diligence)

- 1- All customers shall be subject to CDD measures, taking into account the risks identified by the Licensed Person under Section Second. The only exception to this rule (i.e. reduced measures are applied) is on the basis of lower risk, such as when information on the identity of the customer and beneficial owner is publicly available, in the case where the customer is a company listed on the stock exchange of a country sufficiently implementing the FATF recommendations, or is a subsidiary of such a listed company. However, where such a listed company is subject to the control of an individual or a small group of individuals, a Licensed Person shall carefully review the AML/CFT risks and consider whether it is necessary to verify the identity of such individual(s), be it an owner or a beneficial owner.
- 2- A Licensed Person shall adopt the enhanced CDD measures referred to in these Regulations on higher risk type of customers, business relationships or transactions. These measures vary from case to case depending on the customer's background, type of transactions and circumstances thereof. The Licensed Person must be very cautious in exercising its own judgment when applying these measures to customers of that particular high risk type.
- 3- A Licensed Person must establish clearly in its customer acceptance policies the risk factors for determining the types of customers and activities that are to be considered as high risk. Such risk factors include customer risk, country, geographic risks, product and service risk, and delivery channels risks, without losing sight of other relevant risks.

- 4- In assessing whether or not a country sufficiently applies the FATF AML/CFT standards, the Licensed Person must:
 - a- Assess the standards of prevention of money laundering and terrorism financing. The Licensed Person can rely on the information and data made available on the country concerned by relevant authorities. The higher the risk, the greater the due diligence measures that must be applied when undertaking business with a customer from the country concerned.
 - b- Pay particular attention to assessments of compliance of such country with the FATF recommendations that have been undertaken by the FATF, FATF-style regional bodies, or International Institutions such as the International Monetary Fund or the World Bank.
 - c- Maintain ongoing vigilance concerning money laundering and terrorism financing and take into account information that is available to the Licensed Person about the level of AML/CFT standards in the country concerned where any of its customers operate.
- 5- Apart from the risk factors set out in paragraph (3) of Section Eighth, the following are considered high risk types of customers:
 - a- Complex legal arrangements that have no apparent legal or economic purpose;
 - b- Any person (including companies and other financial institutions) from or in countries which do not or insufficiently apply the FATF recommendations, for example countries designated as such by the FATF;
 - c- PEPs.
- 6- A Licensed Person must perform enhanced due diligence on higher risk customers. Among the measures to be applied as a minimum:
 - a- Obtaining declarations in writing from the beneficial owners about the identity of, and relationship with the directors and substantial shareholders;
 - b- Obtaining additional information on the purpose and reasons for opening the account, business or employment background, source of funds, identification

data of the customer and beneficial owner and on the intend nature of the business relationship;

- c- Assigning staff to serve the customer and those staff must conduct CDD and ongoing monitoring in order to ensure that unusual transactions are analyzed and suspicious transactions are identified on a timely basis;
- d- Conducting face-to-face meetings with the senior management of the customer on a regular basis throughout the business relationship;
- e- Obtaining the approval of the senior management of the Licensed Person when opening an account.

Ninth: Politically Exposed Persons (PEPs)

- 1- The Licensed Person shall have risk management systems in place to identify whether a customer, potential customer or a beneficial owner is a PEP. The Licensed Person shall consider such accounts higher risk and subject them to ongoing and enhanced monitoring.
- 2- If the Licensed Person determines that the customer or beneficial owner is a PEP, it should apply the following additional customer due diligence measures:
 - a- Have the opening or operation of an account for any of the persons mentioned in this Section must be approved by the senior management of the Licensed Person.
 - b- Where a Licensed Person has accepted a customer, and the customer or beneficial owner becomes or is found to be a PEP, the Licensed Person shall obtain the approval of the senior management to continue the business relationship;
 - c- Take measures to establish the source of wealth and source of funds of PEPs or of any person associated with them, who can be a customer or beneficial owner.

- 3- If a Licensed Person determines that a customer or beneficial owner is a domestic PEP or a person who is has been entrusted with a prominent function by an international organization, the measures referred to under (2) above shall be applied wherever the Licensed Person determines the risk of money laundering or terrorism financing to be higher.

Tenth: Non-profit Organizations or Entities

A Licensed Person shall have in place policies, procedures and internal controls to comply with the requirements regarding the opening and handling of accounts and transactions of non-profit organizations and entities. The following requirements shall be observed when dealing with accounts of any such organizations and entities:

- 1- Non-profit organizations and entities must have an official license issued by the relevant government authority specifying the purposes and activities of the organization.
- 2- Due diligence measures shall be applied when dealing with such organizations.

Eleventh: Cases where the Licensed Person must perform CDD

- 1- The Licensed Person must carry out CDD measures when:
 - a- Opening an account or establishing a business relationship;
 - b- There is a suspicion of money laundering or terrorism financing;
 - c- There is doubt about the veracity or adequacy of data, information or documents previously obtained from the customer or beneficial owner for the purpose of verifying his identity.
- 2- A Licensed Person must verify the identity of the customer, potential customer and beneficial owner before and during the course of establishing the business relationship or carrying out the transaction. When the Licensed Person is unable to perform CDD measures satisfactorily at the account opening stage or prior to carrying out the transaction, it must terminate the business relationship and not perform any transaction, and must make a suspicious transaction report (STR). The provision also

applies to existing customer relationships established prior to the enactment of this Instruction.

Twelfth: Collective Investment Schemes

- 1- Where the Licensed Person acts for a customer who is investing in a collective investment scheme, it shall carry out CDD on the customer and comply with the requirements of these Regulations. Except that where the customer is Counterparty, the Licensed Person need not verify the identity of the beneficial owners that are investing through the Counterparty provided that the requirements of paragraph (2) of this Section are met.
- 2- The Licensed Person must ensure that the Counterparty:
 - a- Is regulated and supervised by a competent authority;
 - b- Operates in a country that applies the FATF recommendations;
 - c- Applies, 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 the FATF recommendations;
 - d- Has entered into an agreement with the Licensed Person agreeing to provide the latter or the Authority with any information requested regarding the beneficial owners.

Thirteenth: Reliance on third parties for CDD

- 1- This Section refers to a third party that introduces customers to a Licensed Person and performs customer identification and verification on its behalf. For the purposes of this Section, the third party must either be a commercial bank or a financial institution that engages in securities and is regulated by the CMA.
- 2- The Licensed Person may rely on the third party to apply the requirements of subparagraphs (2) (a) to (c) of the CDD measures of Section Seventh of these Regulations, provided that the criteria set out in Section Thirteenth are met. In all cases, the ultimate responsibility of customer identification and verification always

remains with the Licensed Person and not with the third party, with the application of paragraph (5) of Section Seventh.

- 3- The Licensed Person may rely on third parties to perform CDD if the customer is located in a country other than Kuwait.
- 4- Prior to reliance, the Licensed Person must ensure that it is reasonable to rely on a third party to apply the CDD measures and that these measures are as rigorous as those performed by the Licensed Person for its customers. The Licensed Person must establish clear policies to determine whether the third party in question possesses an acceptable level of reliance.
- 5- The Licensed Person relying on a third part must:
 - a- Obtain from the third party copies of the CDD documentation and information as required by sub-paragraphs (2) (a) to (c) of Section Seventh of these Regulations, including the information referred to in Section Fifth of these Regulations.
 - b- Take adequate steps to ensure that copies of documentation and data relating to the CDD requirements will be made available from the third party upon request. Such documents cover establishing responsibilities in writing or reaching an agreement with the third party whereby the latter commits to, immediately, present and make available all the documentations upon request. The Licensed Person will be then permitted to verify the CDD measures undertaken by the third party at any stage.
 - c- Ensure that the third party is regulated, monitored and supervised by a competent authority, and has measures in place to comply with the customer due diligence and record keeping requirements in line with these Regulations and the FATF recommendations.
- 6- The Licensed Person must conduct quarterly reviews to ensure that the third party continues to conform to the standards set forth in Section Thirteenth. This may

involve reviews of relevant policies and procedures and sample checks of the due diligence conducted.

- 7- The Licensed Person must not rely on third parties based in a country considered as high risk, such as countries that have no or inadequate AML/CFT systems.

Fourteenth: Acquisition

When a Licensed Person acquires, in whole or in part, a financial institution in a foreign country, the Licensed Person shall ensure that the acquired institution has or will perform CDD measures consistent with the requirements of these Regulations at the time of acquisition, by undertaking the following:

- 1- Ensure that the acquired institution holds CDD records for all the customers, including customer identification information, thus precluding any doubts that the Licensed Person might have about the veracity or adequacy of the information acquired.
- 2- Conduct enquiries on CDD measures performed by the acquired institution to ensure the adequacy of such measures and controls with combating money laundering and terrorism financing.

Fifteenth: Non-face-to-face business relationships

- 1- A Licensed Person shall consider money laundering and terrorism financing threats that may arise from the development of new products or business practices, including new delivery mechanisms, and the use of new or developing technologies, and must formulate policies, procedures and internal controls to prevent such threats.
- 2- A Licensed Person must formulate policies, procedures and internal controls that address the risks associated with non-face-to-face business relationships and transactions. Risks arising from the implementation of specific and effective measures during the course of the business relationship should be considered as part of ongoing CDD.

Sixteenth: Ongoing CDD and unusual transactions

- 1- The Licensed Person must monitor on an ongoing basis the business relationship it has with customers, and must ensure that the transactions are consistent with the information the Licensed Person has on the customer's business, risk profile and source of funds.
- 2- The Licensed Person must scrutinize and pay attention to all complex and large transactions and all unusual patterns of transactions which have no economic or visible legal purpose.
- 3- The Licensed Person must scrutinize and pay attention to business relationships or transactions with customers or financial institutions from countries which do not or insufficiently apply the FATF recommendations. Where the Authority advises the Licensed Person that such country insufficiently applies the FATF recommendations, the Licensed Person shall treat all business relationships and transactions from that county as high risk and shall apply the measures set out in paragraph (6) of Section Eighth of these Regulations.
- 4- The Licensed Person must obtain adequate information on the purpose and nature of all transactions, including the examination of transactions that have no economic or visible legal purpose and of findings established in writing, which must be retained for at least 10 years after the date of transaction and made available to the Authority, and internal and external auditors if requested.

Seventeenth: Review and updating of records

Data collected under CDD must be kept up-to-date, accurate and relevant. The Licensed Person must undertake annual or as-needed reviews of existing records, particularly for high risk categories of customers or business relationships when trigger events occur, such as:

- 1- An existing customer applying to open a new account or establishing a new relationship, or significantly altering the nature of the existing relationship;

- 2- When there is a transaction that is unusual or not in line with the customer's normal trading patterns based on the Licensed Person's knowledge of the customer;
- 3- When the Licensed Person is not satisfied that it has sufficient information about the customer or has doubts about the veracity or adequacy of previously obtained data.

Eighteenth: Record keeping requirements

- 1- The Licensed Person shall comply with the record keeping requirements contained in these Regulations and any instructions or guidelines issued by the Authority, and must keep a record of all customer identification data and other previously obtained information and documents, account files, business correspondence, as well as all transactions records.
- 2- The Licensed Person shall maintain sufficient records to permit reconstruction of any transaction, including the amounts and type of currencies involved, so as to provide evidence for prosecution of criminal activity, if necessary.
- 3- The Licensed Person shall keep information regarding the customers' accounts, in particular the following:
 - a- Details of the customer and beneficial owner(s) (if any) of the account, and any other CDD information required;
 - b- Account details, including the volume of funds flowing through the account;
 - c- For transactions, the origin of the funds, the form in which the funds were provided or withdrawn, checks, transfers and others, the identity of the person undertaking the transaction, the destination of the funds, and the instructions – if any – given to carry out such a transfer.
- 4- The Licensed Person shall ensure that all customer and transaction records and information are made available to the Authority upon request.
- 5- The Licensed Person shall maintain records on all domestic and international transactions, whether they have been attempted or already conducted, for at least 10 years from the date of transaction. Such records must be in as much detail as to allow retracing each transaction separately.

- 6- The Licensed Person shall keep all CDD records, account files and business correspondence for at least 10 years after the account is closed.
- 7- The Licensed Person shall keep risk assessments and any information thereof for at least 10 years from the date on which they were conducted or updated.
- 8- In situations where the customer records are subject to ongoing investigations or subject of a suspicious transaction report, they shall be retained until the closure of the case, even if this is still ongoing after 10 years.
- 9- The Licensed 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.

Nineteenth: Suspicious Transaction Report

- 1- The Licensed Person must immediately report to the FIU any activity or transaction that is related or suspected to be related to money laundering, financing of terrorism, terrorist acts, or terrorist organizations.
- 2- The Licensed Person must submit to the FIU along with the STR a detailed report setting out all available data and information about the suspicious transactions and parties involved. The report shall, as a minimum, include the following details:
 - a- Account statements for a period of 6 months,
 - b- Copies of all account opening documents,
 - c- Any data related to the nature of the reported transactions,
 - d- The indications and justifications for the suspicion, along with all supporting documents
- 3- Suspicious transactions must be reported regardless of whether they are related to other suspicious transactions of the customer in question that have already been reported to the FIU.
- 4- The Licensed Person shall appoint a compliance officer at the senior management level to be responsible for the implementation of the provisions of the AML/CFT Law and any relevant laws, and of the requirements of these Regulations. The

Licensed Person shall instruct all staff to promptly refer to the compliance officer any complex, huge, or unusual transaction, or any transaction that raises doubts or suspicion, or any activity that is related or suspected to be related to money laundering, financing of terrorism, terrorist acts, or terrorist organizations in order to take necessary action for referral to the FIU. The Compliance Officer must be a registered and qualified person, and have practical experience in AML/CFT.

- 5- The executive management, including the Compliance Officer with the Licensed Person, shall be concerned with the implementation of reporting procedures to the Kuwait Financial Intelligence Unit. The executive management must play on a regular basis an active role in the identification and reporting of suspicious transactions, and shall review reports of large or irregular transactions generated by the Licensed Person's internal systems, as well as review any reports made by an employee of the Licensed Person.
- 6- In the event any of the employees of the Licensed Person brings a suspicious transaction to the attention of the Compliance Officer, the circumstances of the case shall be reviewed at that level to determine whether the suspicion is justified. If the executive management has decided, based on the recommendation of the Compliance Officer, not to report the transaction to the Kuwait Financial Intelligence Unit, the reasons for this shall be fully documented.
- 7- The Licensed Person must keep records of all transactions referred to the Compliance Officer, together with all internal observations and analysis done in relation to them. A register must be maintained of all suspicious transaction reports made to the Kuwait Financial Intelligence Unit as well as of all the reports made by employees, including suspicious transaction reports that the executive management has decided not to report to the Kuwait Financial Intelligence Unit based on the recommendation of the Compliance Officer.
- 8- The Licensed Person must verify it has received an acknowledgment of receipt from the Kuwait Financial Intelligence Unit for any suspicious transaction report.

- 9- The Licensed Person must continue to monitor the account and the client, and must follow up with the Kuwait Financial Intelligence Unit on the status of the suspicious transaction report if appropriate or in the case where a response is not received from the Kuwait Financial Intelligence Unit regarding a suspicious transaction report.
- 10- Where the Kuwait Financial Intelligence Unit requires further information from a Licensed Person to follow up on a suspicious transaction report, the Licensed Person must provide the information promptly and without delay.

Twentieth: Tipping Off

- 1- In all circumstances, a Licensed Person, its directors, officers and employees are prohibited from disclosing to a customer or any other person the fact that they have made or are considering making a suspicious transaction report or provided or are considering providing any other information related to the unit or any money laundering or terrorism financing investigation to the Kuwait Financial Intelligence Unit. A Licensed Person shall at all times keep its reporting of suspicious transactions highly confidential, and reports that are to be reviewed by the Compliance Officer shall be accessible only by specifically authorized staff of the Licensed Person.
- 2- Whenever a suspicious transaction report has been made to the Kuwait Financial Intelligence Unit 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 suspicious transaction report has been made. The Licensed 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 actions made with regard to the suspicious transaction report.
- 3- The Licensed Person's internal regulations shall stipulate the sanctions applicable to anyone who violates the ban stipulated in sections (1) and (2) above.

Twenty-first: Designated Persons on the United Nations Terrorist List

In accordance with the provisions of Article (25) of Law No. (106) of 2013 AML/CFT, and pursuant to Ministerial Resolution No. (5) of 2014 on the Executive Regulation for the Implementation of United Nations Security Council Resolutions Issued under Chapter (7) of the United Nations Charter Related to Terrorism and Terrorism financing, the Licensed Person must conduct the following:

- 1- Comply with the provisions of the Ministerial Resolution No. (5) of 2014 mentioned above.
- 2- Abide by the provisions of the guidelines issued for the entities concerned with fulfilling the requirements of Ministerial Resolution No. (5) of 2014.
- 3- Set adequate policies and procedures to ensure the implementation of all the obligations mentioned in this Section.

Twenty-second: Internal Policies and Compliance

- 1- The Licensed 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 Licensed Person shall send its internal policies, procedures to the supervisory authority upon request.
- 2- The internal policies and procedures must implement and comply with all relevant regulatory and legal requirements pertaining to AML/CFT and include risk assessment of customers and transactions, CDD measures, record retention, the scrutiny of transactions undertaken throughout the course of the business relationship, the analysis of unusual transactions, the obligation to make a suspicious transaction report to the Unit, and adequate screening procedures to ensure high standards when hiring employees. The internal policies, procedures, systems and controls should be consistent with the Licensed Person's size, and nature and scope of operations and should be adopted by the board of directors of the Licensed Person.
- 3- A Licensed Person shall ensure that the Compliance Officer and any of its staff performing compliance functions may act independently and have timely access to all

client and transaction records and other relevant information which they may require to discharge their functions.

- 4- The Compliance Officer must have appropriate experience and qualifications in field of AML/CFT.
- 5- The Compliance Officer shall undertake the following duties:
 - a- Develop, update and implement the Licensed Person's systems, procedures and controls on AML/CFT.
 - b- Keep pace with developments in AML/CFT laws and regulations, trends, techniques, and update indicators of money laundering or terrorist financing.
 - c- Ensure that the Licensed Person complies with policies and procedures to combat money laundering and terrorist financing.
 - d- Receive directly from staff any reports of suspicious transactions or activities and analyze those reports and then decide whether to file an STR with the Kuwait Financial Intelligence Unit or not.
 - e- Prepare an annual report to the Board of the Licensed Person setting out all actions that have been taken to implement the internal policies, procedures and controls and any proposal for increasing the effectiveness and efficiency of the procedures. A copy of the report shall be submitted to the Authority.
 - f- Ensure that staff of the Licensed Person maintains all necessary records, documents and reports.
 - g- Organize ongoing training programs and plans for all staff of the Licensed Person.

Twenty-third: Audits

- 1- The Licensed Person shall establish an adequately resourced and independent internal audit functions to verify the compliance with the internal policies, procedures, systems and controls and ensure their effectiveness and conformity with the provisions of the Anti-Money Laundering and Terrorist Financing Law and these

Regulations. The internal audit in the Licensed Person shall regularly assess the effectiveness of the Licensed Person's internal AML/CFT policies, procedures and controls.

- 2- The Licensed Person shall have an external audit carried out as prescribed by the CMA. The external auditor shall report on the entity's adherence to all applicable local laws, ministerial decisions and CMA instructions relative to AML/CFT, as well as the person's adherence to its own policies, procedures, systems and controls.

Twenty-fourth: Training

- 1- The Licensed Person must take all appropriate steps to ensure that their staff, directors, board members, and executive and supervisory management members receive regular training on:
 - a- AML/CFT laws and regulations, and in particular, CDD measures, detecting and reporting of suspicious transactions;
 - b- Prevailing techniques, methods and trends to combat money laundering and terrorist financing; and
 - c- The Licensed Person's internal policies, procedures and controls on AML/CFT and the responsibilities of staff in combating money laundering and terrorist financing.
- 2- The Licensed Person must have educational programs in place for training all new and current employees. Refresher training must also be provided at regular intervals to update the staff's information, build their capacities and ensure they are well aware of their responsibilities; in particular those who deal with the public directly and help clients open new accounts.
- 3- When choosing staff, the Licensed Person must ensure that they meet the requirements stated in the Regulations of the Authority on Efficiency and Integrity and ensure that they are qualified and possess a high level of efficiency to enable them to discharge their functions.

Twenty-fifth: Sanctions

Without prejudice to the sanctions imposed under the AML/CFT Law and any other relevant laws, any Licensed Person or any member of the Board, manager or employee of a Licensed Person that fails to comply with any article of these Regulations shall be subject to the sanctions set out in Law No (7) of 2010 on Establishing the Capital Markets Authority and Regulating Securities Activities and its Executive Bylaws.

Twenty-sixth: Publication and Entry into Force

These Regulations shall constitute the minimum requirement to combat money laundering and terrorist financing for Licensed Person and shall become effective upon their publication. They shall replace the Capital Markets Authority Regulations No. (CMA/S.S./I.C./4/2013) on Combating Money Laundering and Terrorist Financing.

Issued on 23/7/2015