Insurance Regulatory Unit **New Kuwait**

Resolution No. (38) of 2021
Regarding the Issuance of Anti-money Laundering and Combating the Financing of Terrorism Rules for Insurance Sector

Chairman, Supreme Committee of Insurance Regulatory Unit,

Having perused:

- Law No. (125) of 2019 regarding the Regulation of Insurance and its Executive Regulations,
- Law No. (106) of 2013 regarding Anti-money Laundering and Combating the Financing of Terrorism and its Executive Regulations, as amended, and
- The Resolution passed by Supreme Committee of Insurance Regulatory Unit in its meeting No. (12) of 2021 held on 31/08/2021 regarding the approval of issuing Anti-money Laundering and Combating the Financing of Terrorism Rules for Insurance Sector,

Resolved as follows:

Article (1)

The Anti-money Laundering and Combating the Financing of Terrorism Rules for Insurance Sector, as attached hereto, shall be issued.

Article (2)

All entities governed by the provisions of Article (2) of Law No. (125) of 2019 regarding the Regulation of Insurance shall regularize their status according to the provisions of Anti-money Laundering and Combating the Financing of Terrorism Rules for Insurance Sector within one year from the publishing date of this Resolution.

Article (3)

The Resolutions passed by the Unit shall continue to be effective unless they are in conflict with the provisions of Anti-money Laundering and Combating the Financing of Terrorism Rules for Insurance Sector, which are attached hereto.

Article (4)

The provisions of Anti-money Laundering and Combating the Financing of Terrorism Rules for Insurance Sector shall come into force effective from the date of publishing this Resolution in the Official Gazette.

Chairman, Supreme Committee
Mohamed Sulaiman Al-Otaibi
Signed/ Stamped

Issued on 01/09/2021

Insurance Regulatory Unit

Anti-money Laundering and Combating the Financing of Terrorism Rules for Insurance Sector

Chapter I: Definitions

Article (1) The following words and expressions used in these Rules shall have the same meanings set forth in the Law and its Executive Regulations and Law No. (106) of 2013 regarding Anti-money Laundering and Combating the Financing of Terrorism and its Executive Regulations, and shall form an integral part of these Regulations. Further, the following words and expressions shall have the meaning assigned thereto, unless the context otherwise requires:

1. Law: Insurance Regulation Law.
2. Unit: Insurance Regulatory Unit.
3. Rules: Anti-money Laundering and Combating the Financing of Terrorism Rules for Insurance Sector.
4. Supervised Entities: Insurance companies, reinsurance companies, Takaful insurance companies, branches of foreign insurance

companies, insurance and reinsurance pools, insurance agents, insurance brokers, reinsurance brokers or any of their Board of Directors members, executive or supervisory management members or managers.

5. Violations: Any act or failure to act resulting in violation of the obligations, controls, regulations or requirements set forth in the aforesaid Law No. (106) of 2013 and its Executive Regulations, these Rules or the IRU resolutions regarding anti-money laundering and combating the finance and terrorism.
6. Compliance Officer: A person appointed by a Supervised Entity, who shall be responsible for implementing the obligations, controls, regulations or requirements set forth in the aforesaid Law No. (106) of 2013 and its Executive Regulations, these Rules or the IRU resolutions regarding anti-money laundering and combating the finance and terrorism.

Chapter II: General Provisions

Business Policies and Procedures

Article (2) The Supervised Entities shall develop the business policies, procedures, systems and

internal controls of anti-money laundering and combating the financing of terrorism in line with the size, nature and scope of operations of the company or insurance pool, provided that the same shall be approved by senior management of the Supervised Entity and applicable to all local and overseas branches and subsidiaries of the Group, if any, and shall ensure that its overseas branches and subsidiaries shall implement the requirements set forth in Article (10) of the aforesaid Law No. (106) of 2013 to the extent permitted by the local laws of host country.

Article (3) If the laws of the host country don't permit the complete application of the requirements stated in the preceding article, the supervised entity shall apply additional adequate measures to manage the risks of anti-money laundering and combating the financing of terrorism and notify IRU of the same.

The supervised entities shall develop mechanisms for exchanging available information and maintaining confidentiality thereof at the level of all local and overseas branches and the subsidiaries of the Group, if any.

Precautionary Measures

Article (4) The supervised entities shall apply the following precautionary measures:

1. Assess the customers and transaction risks;
2. Identify and verify the identity of customer, beneficial owner and politically exposed person;
3. Maintain records and transactions related to customers;
4. Apply due diligence measures to the customer and beneficial owner;
5. Conduct independent inspection and review of the processes of policies, business procedures, systems and internal controls;
6. Appoint Compliance Officer at senior management level, who shall be responsible for implementing the obligations set forth in the aforesaid Law No. (106) of 2013 and its Executive Regulations, these Rules or any resolutions or instructions issued by the IRU or Kuwaiti Financial Intelligence Unit in this regard;
7. Develop high competence criteria for recruiting the employees;

8. Conduct ongoing training programs regarding anti-money laundering and combating the finance and terrorism for all new and existing employees; and
9. Any other requirements set by IRU.

Chapter III: IRU

Article (5) The IRU shall approve efficient training providers to prequalify the Compliance Officer and train the employees of supervised entities considering the following:

1. Conditions for the trainer:
   (1) The trainer shall hold accredited certification permitting them to provide AML-CFT training;
   (2) The trainer shall a member of an international AML-CFT organization; and
   (3) The trainer shall pass the exam prepared by IRU for this purpose.
2. Conditions for training programs:
   a. The academic material of training programs shall be presented to IRU for approval; provided that the same shall include the obligations set forth in the aforesaid Law

No. (106) of 2013 and its Executive Regulations, these Rules and the resolutions, instructions and guidelines issued by the IRU regarding anti-money laundering and combating the financing of terrorism;

b. The training program period shall not be less than five days; and

c. The trainee shall be provided with a certified certificate indicating their commitment to attendance and successfully passing the court exam.

Mechanism for enforcing UN Security Council's Resolutions passed under Chapter VII of UN Charter related to Terrorism and Financing of Terrorism

Article (6) IRU shall specify an electronic medium to receive the data related to individuals on sanctions lists from the concerned authorities both in cases of listing and delisting.

Article (7) Upon receiving any application from a supervised entity, IRU shall verify and review their data and ensure that their names is not listed on the sanctions lists issued by the concerned authorities.

If the applicant for service is listed on the sanctions list, IRU shall stamp the application

with the statement “Contact IRU within one week for AM-CFT purposes”.

Chapter IV: Obligations of Supervised Entities

Electronic Record System

Article (8) The supervised entities shall create electronic record system in which all data of customers and transactions, as defined by IRU, shall be recorded. IRU shall have the authority to access such system online at any time.

New Products and Business

Article (9) The supervised entities shall define AML-CFT risks that may arise from the following processes:

a. Development of new products and business line including the mechanism for offering new products and services; and
b. Deployment of new technologies or those developed for existing and new products.

The supervised entities shall assess such processes, take the necessary measures in this regard and present the same to IRU as and when requested.

Internal Controls and Systems

Article (10) The supervised entities shall:

1. Grant the Compliance Officer and other concerned employees the authority to directly access the customer's identification data, other information related to due diligence measures, transaction records and other relevant information;
2. Senior management will review periodic reports on the requirements of the aforesaid Law No. (106) of 2013 and its Executive Regulations, these Rules and the resolutions, instructions and guidelines issued by the IRU regarding anti-money laundering and combating the financing of terrorism on regular basis. Such report shall include a statement of all suspicious transactions identified and the measures taken by the Compliance Officer to enhance the supervised entity's policies, business procedures, systems and controls;
3. Senior management shall review the findings of any field inspection conducted by IRU including corrective actions to be applied by supervised entities;
4. Carry out independent audits and inspections to verify that the Compliance Officer and

employees of the supervised entity perform their duties in line with internal policies, business procedures, systems and controls related to AML-CFT area;

5. The auditor's report shall include assessment of internal control systems of the supervised entities and extent of their compliance with laws;
6. Requirement of appropriateness, integrity and competence shall be met when recruiting employees, members of executive and supervisory management and managers and upon selecting the members of Board of Directors, in particular:
   a. They shall have high level of competence and integrity to perform their roles; and
   b. Ensure that there are no actual or potential conflicts of interest.
7. Maintain the following records:
   a. Total insurance record;
   b. Compensations record of amounts exceeding K.D. 3,000 per customer; and
   c. Canceled policies record.

Record Retention Requirements

Article (11) The supervised entities shall retain the following documents and information:

1. Copies of all records generated through the due diligence process including the identification documents of customers and real beneficiaries, accounting files and business communications for minimum ten years after the end of business relationship or the date of transaction execution for a customer who has no business relationship with the supervised entities.
2. Copies of all local and international transactions whether already executed or there was an attempt to execute the same, for minimum ten years after the transaction execution or attempt of execution. Such transactions shall be detailed to the extent that allows reconsidering the steps of individual transactions.
3. Copies of notices sent and related documents for minimum ten years after the date of notice submission to Kuwait Financial Intelligence Unit.
4. Copies of information related to risk assessment requested by the IRU for ten years

from the date of conducting or updating the assessment.

Reporting Suspicious Transactions

Article (12) The supervised entities shall report to the Kuwait Financial Intelligence Unit within maximum two working days any transaction or attempted transactions irrespective of the value thereof if they suspect that such transactions are carried out using funds constituting proceeds from a crime or funds relating to AML-CFT operations or can be used for carrying out such operations.

Article (13) The supervised entities and their officers shall not disclose to a customer or third party that a communication with Kuwait Financial Intelligence Unit has been or will be made or existence of AML-CFT investigation. This shall not preclude disclosures or communications between the supervised entities' managers, employees, lawyers, concerned authorities and Public Prosecution. A transaction is particularly considered suspicious in the cases set out in Appendix (1) to these Rules.

Chapter V: Risk Assessment

Article (14) The supervised entities shall assess the association of AML-CFT risks with their business including those related to development of new products and technologies, and maintain and regularly update the risk assessment study and relevant information in writing and submit the same to IRU if it so requests.

Article (15) The supervised entities shall set the appropriate procedures to identify, assess, monitor, manage and mitigate AML-CFT risks, taking the following factors into consideration:

1. Potential risks related to customers;
2. Countries or territories in which customers have carried on their business or source of transactions; and
3. Nature of products and services offered, and transactions and offering mechanism thereof.

Article (16) The supervised entities shall determine the potential factors, which constitute high risk cases and require enhanced due diligence measures, including but not limited to:

1. Risk factors associated with customers:

a. Business relationship taking place in abnormal conditions.
b. Customer not residing in the country.
c. Legal person or legal arrangement that manages third party's assets.
d. Company that has nominal shareholders or bearer shares.
e. Activities that deal in cash or exposed to AML-CFT risks.
f. Company's ownership structure is abnormal or highly complex, and the company doesn't have any clear economic or lawful objects as compared to the nature of its business.
g. Business relationships and transactions not executed in the presence of a customer in person.
h. The entity's business relationships with or in countries defined in item (2) of this Article.
i. Politically exposed persons or those associated with a politically exposed person.
j. Customers that have huge assets or the source of their income or assets is unclear.

2. Geographical or other country risk factors:
    a. Countries classified by reliable sources such as published joint assessment reports or monitoring reports such as countries that don't have adequate AML-CFT regulations.
    b. Countries classified by Kuwait Financial Intelligence Unit as high-risk countries.
    c. Countries that are subject to sanctions, embargoes or similar measures issued, for example, by UN or any other reliable international organization.
    d. Countries classified by reliable sources as countries with high corruption levels or other criminal activities.
    e. Countries or territories classified by reliable sources as countries that provide financing or support to terrorist activities or specific terrorist organizations are active within their territories.

3. Risk factors associated with products, services or transactions and offering mechanism:
    a. Anonymous transactions, which would involve cash amounts.

b. Transactions made with a customer who is not present in person for identification purposes.
c. Payments received from anonymous party or a party that has known relationship with the receiving party.

Article (17) The supervised entities shall apply the assessment criteria as per Article (14) of these Rules through adopting the following risk management measures:

1. Risk factors assessment including the following:
   a. Purpose of relationship.
   b. Size of transactions undertaken by a customer.
   c. Frequency of transactions or duration of relationship.
2. Obtain additional information about the customer, beneficial owner, beneficiary and transaction.
3. Develop customer and transaction risk policies on, which are based on adequate information about the customer and beneficial owner, if any, including the anticipated business relationship with supervised entities and the

customer's source of funds and assets, as applicable.

4. Apply the enhanced due diligence measures to high-risk customers.
5. Regularly and accurately update the information of all customers.
6. Adopt any other measures determined by the IRU or Kuwait Financial Intelligence Unit.

Chapter VI: Identification Requirements

Article (18) The supervised entities shall not establish business relationships with anonymous customers or with fictitious names and shall identify and verify the identity of the customer or beneficial owner in the following stages:

1. Before undertaking any transaction with the customer.
2. Before undertaking any transaction exceeding KD 3 thousand or equivalent in a foreign currency with a customer who doesn't have business relationship with the supervised entities whether in a single transaction or series of transactions in one day.
3. In case of suspecting transactions involving money laundering or financing of terrorism.

4. In case of suspecting correctness or adequacy of a customer's identification data previously obtained.

Article (19) The supervised entities shall obtain, as the case may be – valid documents in order to determine the identification of customer or beneficial owner, which are as follows:

1. Civil ID Card for citizens and residents;
2. Passport or travel document for non-residents of Kuwait;
3. Business license issued by Ministry of Commerce & Industry for companies and businesses registered in Kuwait or documents issued by relevant authorities in the other countries for branches of overseas companies and businesses;
4. Documents, papers and court judgments proving that they are the legal representative of the concerned person; and
5. Certified identification documents attested by the relevant official authorities or organizations issuing such documents for customers who don't fall under the scope of the above paragraphs of this Article.

Article (20) The supervised entities shall take the required due diligence measures for the customer, beneficiary and beneficial owner of life insurance or investment related insurance policies immediately upon determining the identity of the beneficiary or beneficial owner as follows:

1. Obtain name for the beneficiary designated as natural or legal person or legal arrangement.
2. Obtain adequate information about the beneficiary to enable the supervised entities to verify the identification of beneficiary when paying the compensation, for a beneficiary designated in certain category such as spouse or children upon occurrence of the insured event or through other means such as will; and
3. Consider the beneficiary of insurance policy referred to in this Article as a high-risk factor associated with the transaction, which requires applying enhanced due diligence measures including taking reasonable measures to determine and verify the identity of beneficiary or beneficial owner at the time of payment.

Chapter VII: Politically Exposed Persons

Article (21) The supervised entities shall develop appropriate risk management systems to determine if a customer or beneficial owner is a politically exposed person.

The measures for identifying the politically exposed person, whether a customer or beneficial owner, shall include the following:

1. Requesting relevant information from the customer;
2. Referring to available customer's information; and
3. Referring to electronic databases related to business affairs of a politically exposed person, if available.

Article (22) If a customer or a beneficial owner is determined to be a politically exposed person, the supervised entities shall apply the following additional due diligence measures:

1. For a foreign politically exposed person:
   a. Obtain the approval of senior management before establishing or continuing the business relationship with such person;
   b. Take all appropriate measures to determine the source of funds and assets; and

c. Apply enhanced ongoing monitoring of the business relationship.

2. For a local politically exposed person, the above measures shall be applied if it is found that the AML-CFT related risks, as defined by the supervised entities, which are associated with such person are high.

Article (23) The supervised entities shall take reasonable measures to determine whether or not a beneficiary or beneficial owner is a politically exposed person.

If the supervised entities conclude that the beneficiary or beneficial owner is a politically exposed person, they shall notify senior management before exercising any rights related to insurance policies or before paying due compensations for the insurance policy related to protection and/or savings or the investment-related insurance policies; conduct a thorough inspection regarding the business relationship; and consider reporting suspicious transactions to Kuwait Financial Intelligence Unit.

Chapter VIII: Customers and Beneficiaries

Customer Acceptance

Article (24) The supervised entities shall refrain from establishing business relationship or executing a transaction if it is impossible to verify the identity of the customer or beneficial owner, and shall notify Kuwait Financial Intelligence Unit.

Retention of customer's information

Article (25) The supervised entities shall gather information about the customer and beneficial owner and retain the same for minimum ten years. Further, the data and information gathered in the course of due diligence measures shall be updated along with verifying the validity thereof through reviewing the existing records within the grace period set by the IRU.

Ongoing monitoring of customer's transactions

Article (26) The supervised entities shall monitor the customers' transactions on ongoing basis, including the following:

1. Audit the customers' transactions to verify that the same are executed based on the supervised entities' knowledge of the customer, their risk profile and sources of funds and assets; and
2. Monitor the predetermined restrictions on amounts, size and type of transactions.

Termination of relationship with a customer

Article (27) The supervised entities shall terminate the relationship with the customer and notify the IRU if they are unable to verify the identity of beneficial owner in the course of business relationship, or if it is impossible for them to comply with the required due diligence measures towards the customer.

Determination of beneficial owner

Article (28) The supervised entities shall take the necessary measures to determine if a customer acts on behalf of one or more real beneficiaries through obtaining a declaration signed by the customer upon executing the transaction indicating that the customer doesn't act or execute the transaction on behalf of another person or through any other sources.

Article (29) If the supervised entities find out that a customer acts on behalf of the beneficial owner, they shall:

1. Verify the identity of the beneficial owner by using the relevant information or data obtained from a reliable source confirming the identity of beneficial owner; and

2. Apply due diligence measures that are commensurate with risks associated with the beneficial owner or beneficiaries in this case.

Article (30) The supervised entities shall only obtain the customer's identification documents if the customer is a legal person and they shall not be required to determine and verify the identity of its shareholders or real beneficiaries if the customer is listed on the stock exchange, provided that the customer shall be subject to transparency and disclosure rules, which disclose the identity of beneficial owner.

Article (31) If the customer is a legal person or legal arrangement, the supervised entities shall take the appropriate measures to understand the customer's ownership and control structure including the beneficial owner holding or controlling it as follows:

1. For legal persons, the beneficial owner of legal person shall be:
   a. Any status, agreement or ownership of shares or interests, whether individual ownership or ownership through affiliate or allied parties, exceeding 25% of shares or interests, or if it controls the appointment

of majority of board members or the director, as the case may be, or the resolutions passed by it or the general meeting of the concerned company.

b. Beneficial owner shall be tracked through any number of legal persons or legal arrangement of any type.

c. If all possible means are utilized and a natural person possessing ultimate controlling ownership as set out in item (a) of this Article can not be identified or if there is doubt that the natural person who has controlling ownership is the beneficial owner, then the natural person exercising the control over the legal person through other means shall be the beneficial owner.

d. If no natural person is identified as stated in the preceding item of this Article, then the beneficial owner shall be the real person who holds the position of senior management officer.

2. For legal arrangements, the identity of the settlor, trustee or any other person entrusted with similar roles of the beneficial owner as

stated in paragraph (1) of this Article shall be verified.

Engagement of third parties

Article (32) The supervised entities may engage third parties to perform certain due diligence measures provided that they shall meet the following requirements:

1. IRU approval
2. Required information about due diligence measures can be accessed in real time.
3. Ensure that the third party shall provide, immediately upon request, a copy of identification data and other documents related to due diligence measures.
4. Ensure that the third party complies with the requirements of due diligence and record retention.

In all cases, the supervised entities shall be responsible for determining and verifying the customer's identity.

Chapter IX: Enhanced Due Diligence Measures on High-risk Customers

Article (33) The supervised entities shall take the enhanced due diligence measures based on the risks

identified in situations where money laundering or financing of terrorism risks are high including politically exposed persons and customers who don't interact face-to-face.

The enhanced due diligence measures shall be applied to high-risk customers on ongoing basis in each of the due diligence process stages as long as the relationship wit the customer still exists.

Article (34) The supervised entities shall examine complex and abnormal transactions and verify the purpose thereof and all patterns of abnormal transactions for which there are no clear economic or legal purposes.

Article (35) The supervised entities shall intensify the degree and nature of oversight of the transaction to determine if such transaction is abnormal or suspicious.

The enhanced due diligence measures applied to high-risk transaction shall include but not limited to:

1. Obtaining additional information about the customer such as the profession, size of assets and available information thereof, and regularly updating the data of customer and beneficial owner.

2. Obtaining additional information about the nature of anticipated transaction.
3. Obtaining information about sources of the customer's funds or assets.

Obtaining information about reasons behind anticipated or already executed transactions.

Article (36) The enhanced due diligence measures for a customer who is not present in person – for identification purposes, shall include the following:

1. Attestation of the documents as per the relevant laws and procedures.
2. Requesting any additional documents and setting any independent procedures to verify the customer's identity and/or contact with them.

Chapter X: Compliance Offer

Appointment of Compliance Officer

Article (37) The supervised entities shall appoint a senior management level compliance officer who shall be responsible for implementing the requirements of the aforesaid Law No. (106) of 2013 and its Executive Regulations, these Rules or the IRU resolutions regarding anti-money

laundering and combating the finance and terrorism.

The supervised entities may establish a compliance unit, which shall report to senior management and shall be headed by the compliance officer appointed at senior management level.

Further, the supervised entities shall provide the IRU with the details of compliance officer including their name, qualifications, telephone number and email address.

Change of compliance officer

Article (38) The supervised entities shall notify the IRU if the compliance officer is changed, update the necessary data and submit a new certificate as per the requirements of Article (40) of these Rules.

Conditions for appointment of compliance officer

Article (39) The supervised entities shall observe the following conditions upon appointing the compliance officer:

1. The compliance officer's age shall be minimum 21 calendar years.
2. He/she shall not be previously sentenced to a criminal penalty or convicted of honor or trust breaching crime unless they are rehabilitated.

3. He/she shall have minimum bachelor's degree from an accredited university in any of the following majors:
   a. Law
   b. Business administration
   c. Accounting
4. He/ she shall pass the exam prepared by the IRU for this purpose.

He/ she shall hold an accredited training course from the training providers approved by the IRU as per Article (5) of these Rules.

Submission of certificate of compliance offer appointment

Article (40) The supervised entities shall submit to the IRU a certificate issued by Public Authority for Manpower evidencing the appointment of compliance offer.

Roles of compliance officer

Article (41) In the course of performing their roles, the compliance officer shall be independent and report to senior management. He/ she shall oversight the implementation by the supervised entities of the requirements of the aforesaid Law No. (106) of 2013 and its Executive Regulations, these Rules or the IRU resolutions regarding anti-

money laundering and combating the finance and terrorism, particularly:

1. Oversight the implementation of policies, business procedures and internal systems and controls related to AML-CFT and prepare a report on the same, which will be submitted to senior management and the IRU, if requested.
2. Oversight the implementation of requirements of assessment and update of customer and transaction risks and submit the same to the IRU if requested.
3. Review the suspicion red flags of the supervised entities and notify senior management in order to report the suspicious transactions to Kuwait Financial Intelligence Unit and keep the notices for submission to the IRU if requested.
4. Oversight and follow up compliance with the provisions of Article (25) of the aforesaid Law No. (106) of 2013 and compliance with Ministry of Foreign Affairs resolutions issued in connection with AML-CFT.
5. Ensure that records, transactions and studies are maintained and submitted to the IRU if requested.

6. Oversight the implementation of enhanced and due diligence measures on customers and beneficial owner.
7. Provide technical opinion regarding suspicious transactions.

Perform any other tasks assigned to them by senior management or the IRU regarding AML-CFT.

Chapter XI: Judicial Police Officer, Penalties and Legal Measures

Granting and renewal of judicial police officer status

Article (42) Subject to Article (78) of the Law, the following criteria shall be met for granting the judicial police officer status:

1. He/she shall be employee of the IRU.
2. He/she shall hold university degree, diploma or equivalent in any of the following majors:
   a. Law
   b. Business administration
   c. Accounting
3. He/she shall not be previously sentenced to a criminal penalty or convicted of honor or trust breaching crime unless they are rehabilitated.

4. He/she shall pass approved qualifying training course in AML-CFT domain.
5. In case of renewal of judicial police officer status, their annual competence appraisal shall be excellent as minimum.

Loss of judicial police officer status

Article (43) The judicial police officer status shall cease to exist if the holder thereof loses any of the conditions set forth in the preceding Article.

Penalties and Legal Measures

Article (44) Without prejudice to criminal liability set forth in the aforesaid Law No. (106) of 2013, the supervised entities shall be penalized if they commit a violation. The Disciplinary Board may apply one or more measures or penalties for any violation as follows:

1. Issue written warnings of the violation.
2. Issue an order requiring compliance with specific procedures.
3. Issue an order to submit regular reports on the measures taken to rectify the designated violation.
4. Apply financial penalty not exceeding Kuwaiti Dinars five hundred thousand for reach violation.

5. Prevent the offender from engaging in the relevant business for a period to be specified by the Disciplinary Board.
6. Restrict the powers of members of Board of Directors, members of executive or supervisory management, directors and controlling owners including the appointment of a temporary controller.
7. Terminate or request changing the members of Board of Directors, members of executive or supervisory management or directors.
8. Suspend, restrict or prohibit the practice of business, activity or profession.
9. Suspend the license.
10. Withdraw the license.

The Disciplinary Board may apply any other measures as per the Law and its Executive Regulations.

The IRU may add other measures and penalties to the supervised entities for non-compliance with the obligations, controls, regulations or requirements set forth in the aforesaid Law No. (106) of 2013 and notify Kuwait Financial Intelligence Unit of the same.

Anti-money Laundering and Combating the Financing of Terrorism Rules for Insurance Sector

Appendix (1)
Red Flags of Suspicious Transactions

First: Customer-related Red Flags

1. The reason calling a customer to select the supervised entities or branch to execute the transaction is not understood.
2. Unexpected or frequent change of beneficial owner and/ or beneficiaries.
3. Unexpected or frequent change of customer's contact details.
4. The customer uses an address with continuing change of names associated with it.
5. The customer intentionally provides false, misleading, missing or unclear information or refrains from providing the necessary information and documents indicating the business relationship and relevant activity and explaining the source and destination of funds and the purpose of the transaction.
6. The customer attempts avoid or refuses the supervised entities' attempts to contact them personally.
7. The customer refuses sending any documents by the supervised entities to their home address.
8. The customer requests freedom of act exceeding normal scope.

9. Any indicators of business undertaking by the customer, which is penalized under law in the State of Kuwait or other countries.
10. The customer acknowledges their involvement in criminal activities.
11. The customer appears to be abnormally curious about the internal regulations, control, processes, policies and monitoring.
12. The customer over-justifies or overexplains the transaction or extraordinarily provides documents proving validity thereof.
13. The customer is inappropriately tensioned considering the nature of transaction.
14. The customer attempts to build a close relationship with employees.
15. The customer uses assumed names and set of close but different addresses.
16. The customer offers money, rewards, or abnormal services to secure services, which seem abnormal or suspicious.
17. The customer frequently buys insurance policies and then cancels the same shortly.
18. Business relationships with legal persons not listed in the public records or official databases and official certificates can not be obtained about them.
19. When conducting personal discussions, the customer is always accompanied by persons whose job or role is unclear and undertake influential role in creating the business relationship.

20. The customer provides contract details that are inconsistent with the contract details (address, telephone number) of their permanent residence address.
21. The customer accepts adverse conditions that are not relevant to their health or age.
22. The customer requests insurance that doesn't have specific purpose and feels hesitant to disclose the reasons for making this investment.
23. The customer changes the specified beneficiaries (particularly if it is possible to do so without knowing the insurer or their approval and/or transferring the payment right upon signing endorsement of the policy).
24. During the validity of insurance contract, the ultimate beneficiary is replaced with a person who seemingly has no link with the policyholder.
25. The customer doesn't pay attention to policy performance but pays significant attention to early termination of the contract.
26. The customer requests making one payment through wire transfer or in foreign currency.
27. The customer is hesitant to provide normal information when applying for insurance policy, rather the customer gives insignificant or false information or information that is difficult to be verified by the organization or entails high costs of verification thereof.

28. The customer seems to have insurance policies with several organizations.
29. The customer buys insurance policies for amounts that seem to exceed their apparent resources.
30. The customer enters into huge insurance policy within short period and then cancels it and requests refund in cash to be paid to a third party.
31. The customer is willing to borrow the maximum limit of cash value of single premium insurance policy after short period from settling its price.
32. The customer uses postal address outside the area of insurance regulator and during the verification process, it is found that their home phone number is disconnected.
33. Legal persons whose ultimate beneficiary or controlling parties thereof are difficult to be identified. (Note: this can occur at the beginning or at any time thereafter. Further, beneficiary of individually held insurance policy can be changed to a legal person).
34. Medium or low-income professionals who make large continuing deposits with respect to insurance policy.
35. Customers who are hesitant to provide specific information when purchasing a product or provide seemingly simple or false information.
36. The customer transfers the insurance policy to another insurer (from low risk insurance policy within previous long period to

a higher risk insurance policy along with paying higher charges).

37. The supervised entities find out, upon requesting the cancellation, that the beneficiary is changed and the customer assumes high cost due to early termination of the insurance.
38. The customer requests changing or increasing the insured amount and/or pays the insurance premium in abnormal or excessive manner.
39. Accountants, lawyers or other professionals who have accounts/ policies/ contracts with an insurer do business on behalf of their customers and the supervised entities unjustifiably rely on them.
40. Customers who designate or change the beneficiary of policy to a third party who is not associated with them.
41. The customer subscribes for any of the high cost insurance contracts and pays such costs from foreign accounts.

Second: Transaction-related Red Flags

1. Customer's purchases or transactions seem to have no economic purpose.
2. The transaction seems to be inconsistent with the customer's financial position or normal pattern of activities.
3. The transaction seems to be beyond normal scope of business practices in the relevant sector or doesn't seem to be economically viable for the customer.

4. The transactions are complex without cause given the stated objective thereof.
5. Shortage in information or delay in providing the information to allow verification thereof.
6. Occurrence of abnormal event in prepayment of insurance premiums.
7. The customer executes a transaction that results in explicit increase in investment holdings.
8. Any transaction involving unknown party.
9. Requesting implementation of huge purchase of a contract for total amount under which the policyholder has been used to make small and regular payments.
10. Attempts to use cheques from a third party to make a proposed purchase of insurance policy.
11. Payments are regularly made by third parties who don't have clear relationship with the policyholder.

Third: Red Flags related to product/ service/ channels utilized

1. Products purchased are not in line with the experience that a supervised entity has with the customer and the objective of the business relationship.
2. High single-premium insurance policies, particularly those related to repurchase before maturity.

3. Insurance policies with legal persons or legal arrangements serving assets management associated with additional risk factors such as international interventions.
4. Insurance policies with premiums exceeding the customer's apparent resources.
5. Insurance policies with values that seem inconsistent with the customer's insurance needs.
6. Early termination of a product particularly with loss or where cash money is offered and/ or refund cheque is addressed to a third party.
7. Assignment of benefit from a product to a third party who seems to have no clear link with them.
8. Time period of life insurance contract is less than three years.

Fourth: Geographical location-related Red Flags

1. Submit request for obtaining insurance policy by a potential customer whose permanent residence address is not located in the State of Kuwait and has no logical economic relations with the State of Kuwait.
2. The request is submitted by an agent/ broker in non-regulated or poorly regulated territory or where corruption or organized crimes prevail (such as drug trafficking or terrorist acts).
3. The transaction involves usage or payment of performance bond resulting in transborder payment (wire transfers) where the first

(single) premium is settled from a bank account outside the country.