

**CABINET RESOLUTION NO. (134) OF 2025
REGARDING THE EXECUTIVE REGULATIONS
OF FEDERAL DECREE BY LAW NO. (10)
OF 2025 ON ANTI-MONEY LAUNDERING,
COMBATING THE FINANCING OF TERRORISM
AND PROLIFERATION FINANCING**

Cabinet Resolution No. (134) of 2025
Regarding the Executive Regulations of Federal Decree by Law No. (10) of
2025 Regarding Anti-Money Laundering, and Combating the Financing of
Terrorism and Proliferation Financing

The Cabinet:

- Having reviewed the Constitution;
- Federal Law No. (1) of 1972 Regarding the Competences of the Ministries and the Powers of Ministers, as amended;
- Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing;
- Cabinet Resolution No. (10) of 2019 Regarding the Executive Regulations of Federal Decree by Law No. (20) of 2018 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Illegal Organizations, as amended;
- Upon the proposal of the Minister of Finance, and the approval of the Cabinet;

Hereby resolves as follows:

Chapter One

Definitions

Article (1)

The definitions set forth in Federal Decree by Law No. (10) of 2025, referred to hereinabove, shall apply to this Resolution. In addition, the following terms and expressions shall have the meanings assigned to each of them, unless the context requires otherwise:

Companies : Companies, regardless of their type or activity, that are subject to the provisions of the legislation in force in the State.

- Senior Management** : The person or persons vested with authority to take strategic and executive decisions materially affecting risk management, compliance policies, and operational governance, including chief executive officers, general managers, members of the board of directors, or any person occupying a position that enables them to directly influence the conduct of business and internal policies, including compliance policies.
- Intermediary Financial Institution** : A Financial Institution that, in the payment chain, receives and transmits a funds transfer between the originating Financial Institution and the Beneficiary Financial Institution, or another Intermediary Financial Institution.
- Beneficiary Financial Institution** : The Financial Institution that receives the transfer from the originating Financial Institution, either directly or through an Intermediary Financial Institution, for the benefit of the Beneficiary, and which constitutes the end point in the payment chain.
- Financial Institutions** : Any person engaging in one or more financial activities or operations for the benefit of, or on behalf of, a Customer, as stipulated in Article (2) of this Resolution.
- Designated Non-Financial Businesses and Professions (DNFBPs)** : Any person engaging in one or more commercial or professional activities or businesses for the benefit of, or on behalf of, a Customer, as stipulated in Article (3) of this Resolution.

- Commercial Gaming** : Any game of chance, or any form of chance-based or skill-based practice, involving the placement of a monetary stake for the purpose of winning money or any other item of value, including agreements whereby the loser must compensate the winner with money or any other agreed consideration. This includes, without limitation, lottery operations, Commercial Gaming halls, internet gaming, sports wagering, and any other licensed games of chance or opportunity regulated by the General Commercial Gaming Regulatory Authority, whether conducted within gaming premises or elsewhere.
- Commercial Gaming Operators** : Any person who carries out the operation of Commercial Gaming halls, internet Commercial Gaming, sports betting, or lottery gaming.
- Virtual Asset Service Providers** : Any person who, as a commercial activity, conducts one or more Virtual Asset activities or related operations for the benefit of, or on behalf of, another natural or legal person, as stipulated in Article (4) of this Resolution.
- Trust Protector** : A natural or legal person appointed pursuant to a Trust deed and granted powers and authorities for the purpose of protecting the Trust, ensuring its proper administration, and achieving its objectives, without such powers prejudicing its legal independence or resulting in the transfer of assets to the benefit of the settlor, or the settlor's effective control over them.
- Nominator** : One or more natural or legal persons who issue instructions, directly or indirectly, to a nominee acting on their behalf as a Nominee Director or Nominee Shareholder of a legal person.

- Nominee Shareholder** : A natural or legal person who exercises voting rights in accordance with the instructions of the Nominator, or receives dividends on their behalf, and shall not be deemed the Beneficial Owner of a legal person by virtue of holding shares in a nominee capacity.
- Nominee Director** : A natural or legal person who customarily performs management functions in a company on behalf of the Nominator and in accordance with their instructions, and shall not be deemed the Beneficial Owner of a legal person.
- Beneficial Owner** : The natural person who owns or exercises ultimate effective control over the Customer, or the natural person on whose behalf Transactions are conducted, including any natural person exercising ultimate effective control over a legal person or Legal Arrangement, whether directly or through a chain of ownership or control or by any other indirect means, and who is identified, whether one or more persons, in accordance with Article (10) of this Resolution.
- Reasonable Measures** : Measures taken within the framework of Customer Due Diligence and Beneficial Owner identification procedures, proportionate to the risks of Money Laundering, Financing of Terrorism, or Proliferation Financing.
- Business Relationship** : Any ongoing commercial or financial relationship established between Financial Institutions, DNFBPs, or Virtual Asset Service Providers and their Customer, in connection with the activities or services they provide to the Customer.

- Correspondent Banking Relationship** : A relationship between a correspondent Financial Institution and a respondent institution through a current account, or any other type of account or related service, including correspondent relationships established for securities transactions or funds transfers.
- Payable-Through Accounts** : Correspondent accounts used directly by third parties to conduct transactions on their behalf.
- Financial Group** : A group of Financial Institutions consisting of a holding company or another Legal Person that exercises control over the rest of the group, and coordinates functions for the purpose of applying supervision at the group level, across its branches and subsidiaries, in accordance with International Core Principles for Financial Supervision and the anti-money laundering and combating terrorism financing policies and procedures.
- International Core Principles for Financial Supervision** : The Basel Committee’s Core Principles for Effective Banking Supervision (Principles 1–3, 5–9, 11–15, 26, and 29); The International Association of Insurance Supervisors Core Principles (Principles 1, 3–10, 18, 21–23, and 25); The International Organization of Securities Commissions Principles (Principles 24, 28, 29, and 31) and Responsibilities (A, B, C, and D).
- Wire Transfer** : Any operation for the electronic funds transfer conducted by a Financial Institution or a Virtual Asset Service Provider on behalf of an originator, whereby funds are transmitted to a specified Beneficiary at another Financial Institution, Virtual Asset Service Provider, or virtual wallet, whether the originator and beneficiary are the same person or different persons.

- Shell Bank** : A bank incorporated or licensed in a jurisdiction in which it has no physical presence, and is not affiliated with a regulated Financial Group.
- Population Register** : The State Population Register, which includes individual data and civil events, as regulated by Federal Law No. (9) of 2006 Regarding the Population Register and Identity Card System, as amended.
- High-Risk Customers** : Customers who present heightened risk due to their personal profile, activities, the nature of the Business Relationship, or geographic location, including customers from high-risk countries, non-residents not holding a State-issued identity card, customers with complex ownership structures, customers conducting complex or economically or legally unjustified Transactions, customers engaging in large cash Transactions, Transactions with unknown third parties, or any other high-risk Transactions as determined by Financial Institutions, DNFBPs, Virtual Asset Service Providers, or the Supervisory Authority.

Politically Exposed Persons (PEPs) : Natural persons entrusted with, or have been previously entrusted with, prominent public functions in the State or in any other country, such as Heads of State or Government, senior politicians, senior government officials including judicial or military officials, senior executive managers of state-owned enterprises, senior political party officials, and persons entrusted with, or have previously been entrusted with, the management of international organizations or any prominent function therein, including members of Senior Management such as directors, deputy directors, members of the board of directors, or persons of equivalent positions. This definition includes:

1. Immediate family members of the politically exposed person, such as spouses, children and their spouses, and parents;
2. Persons known to be close associates of the politically exposed person, including:
 - a. Persons having joint beneficial ownership of a legal person or Legal Arrangement, or any other close professional or social relationships with a PEP;
 - b. Persons having sole beneficial ownership of a legal person or Legal Arrangement that has been established for the benefit of a PEP.

Adequate Information : In the context of legal persons; information that is available or can be obtained to identify the Beneficial Owner and the means by which ownership or control is exercised, including full name, nationality, date and place of birth, residential address, identity number and type, tax registration number, if any, and any other information required for this purpose. In the context of Legal Arrangements; information used to identify the natural persons who are the Beneficial Owners thereof and their roles, including information on the Trustee, Settlor, Protector, if any, Beneficiary, or, as the case may be, class of Beneficiaries and the authorities and powers granted thereto, and any other person exercising ultimate effective control over the Legal Arrangement or occupying a similar or equivalent position.

- Accurate Information** : Information that has been verified for accuracy. In the context of legal persons; information that has been verified to confirm its accuracy through the verification of the identity and status of the Beneficial Owner using original documents, data, or information obtained from a reliable and independent source. The extent of the verification measures may vary according to the identified level of risk. Where there is a discrepancy in the information, necessary supplementary measures shall be taken to confirm the accuracy of the Beneficial Owner’s information. In the context of Legal Arrangements, information that has been verified to confirm its accuracy through the verification of the identity and status of the Beneficial Owner, using reliable documents, data, or information. The extent of verification measures may vary according to the identified level of risk. Where there is a discrepancy in the information, necessary supplementary measures shall be taken to confirm the accuracy of the Beneficial Owner’s information.
- Up-to-Date Information** : In the context of legal persons, information that is as current as possible and updated within a reasonable, specified timeframe following any change. In the context of Legal Arrangements, information that is as current as possible and updated within a reasonable timeframe. However, where Beneficiaries are designated by characteristics or class, Trustees or persons in equivalent or similar positions are not required to obtain complete Adequate and Accurate Information until a Beneficiary becomes entitled at the time of payment or seeks to exercise vested rights, in accordance with the risk-based approach.

Decree by Law : Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing.

Chapter Two

Financial Institutions, Designated Non-Financial Businesses and Professions, Virtual Asset Service Providers, and Non-Profit Organizations

Part One

Financial Institutions and Designated Non-Financial Businesses and Professions

Division One

Nature of Financial Institutions and Designated Non-Financial Businesses and Professions

Article (2)

Financial Institutions shall include any person who, as a commercial activity, carries out one or more of the following financial activities or operations for the benefit of, or on behalf of, a Customer:

1. Acceptance of deposits and other repayable funds from the public.
2. Lending, including consumer loans and mortgage loans, with or without recourse, and the financing of commercial transactions, including the purchase of export documents and the purchase of debts, whether with or without recourse.
3. Financial leasing, excluding financial leasing related to consumer products.
4. Money or value transfer services, excluding any natural or legal person who solely provides Financial Institutions with messaging or other support systems for the transfer of funds.
5. Issuance and management of means of payment, including debit cards, credit cards, cheques, payment orders, banker drafts, and electronic money.
6. Guarantees and financial commitments.

7. Trading in financial market instruments such as cheques, bills of exchange, certificates of deposit, derivatives, and others; or foreign exchange, currency exchange instruments, interest rates, indices, other financial derivatives, or tradable financial instruments; and trading in commodity futures contracts.
8. Participation in the issuance of securities and the provision of financial services related to such issuances.
9. Management of funds and portfolios of all types.
10. Safekeeping and administration of cash or liquid securities on behalf of others.
11. Other operations for investing, managing, or operating funds or monies on behalf of others.
12. Subscription to, or savings in, life insurance policies and other types of investment-related insurance, including those provided by insurance agents and brokers.
13. Money or currency exchange.
14. Any other financial activities or operations as may be determined by a resolution issued by the Supervisory Authority, in coordination with the National Committee.

Article (3)

Designated Non-Financial Businesses and Professions (DNFBPs) shall include any person who carries out one or more of the following commercial or professional activities or businesses:

1. Commercial Gaming Operators, including Commercial Gaming conducted on board vessels or marine craft, when conducting a single financial transaction or several transactions that appear to be linked and whose value equals or exceeds eleven thousand dirhams (AED 11,000).
A financial transaction shall not include a transaction that solely involves gaming chips or gaming instruments.
2. Real estate brokers and agents, when concluding transactions or settlements on behalf of their customers in relation to the purchase or sale of real estate.

3. Dealers in valuable metals and precious stones, when carrying out any single cash transaction or several transactions that appear to be linked and whose value equals or exceeds fifty-five thousand dirhams (AED 55,000).
4. Lawyers, notaries, other independent legal professionals, and independent accountants, whether practicing individually, as partners, or as professionals within a firm practicing such profession, when they prepare, conduct, or execute financial transactions on behalf of their customers in relation to the following activities:
 - a. Buying and selling real estate;
 - b. Managing funds owned by the customer ;
 - c. Managing bank accounts, savings accounts, or securities accounts;
 - d. Organizing contributions for the establishment, operation, or management of Companies;
 - e. Establishing, operating, managing legal persons or Legal Arrangements, or selling, or purchasing commercial entities.
5. Company and Trust Service Providers, when carrying out or executing any transaction for the benefit of, or on behalf of, their customers in relation to the following activities:
 - a. Acting as an agent in the incorporation or establishment of Legal Persons;
 - b. Acting, or arranging for another person to act, as a director or secretary of a company, or as a partner or in a similar position in another Legal Person;
 - c. Providing a registered office, business address, place of residence, correspondence address, or administrative address for a company, any legal person, or a Legal Arrangement;
 - d. Acting, or arranging for another person to act, as a Trustee of an express Trust or performing an equivalent function for another form of Legal Arrangement;
 - e. Acting, or arranging for another person to act, as a Nominee Shareholder for another person.
6. Any other businesses or professions may be determined by a resolution issued by the Supervisory Authority, in coordination with the National Committee.

Article (4)

Virtual Asset Activities shall include the following activities or operations:

1. Exchange between Virtual Assets and fiat currencies.
2. Exchange between one or more types of Virtual Assets.
3. Transfer of Virtual Assets.
4. Safekeeping or administration of Virtual Assets or instruments enabling control over Virtual Assets.
5. Provision of financial services or activities related to an issuer's offer or sale of Virtual Assets, or participation therein.
6. Any other activities or operations as may be determined by a resolution issued by the Supervisory Authority, in coordination with the National Committee.

Division Two

Risk Identification and Risk Mitigation

Article (5)

1. Financial Institutions, DNFBPs, and Virtual Asset Service Providers shall identify, understand, manage, and assess their crime risks in a manner proportionate to the nature and size of their business, taking into account the risk-based approach and the results of the National Risk Assessment, and shall comply with the following:
 - a. Consider all relevant risk factors, such as Customer risks, countries and geographic risk, product, service, transaction, and delivery channel risks, prior to determining the overall level of risk and the appropriate level of risk mitigation measures to be applied.
 - b. Document the processes for identifying and assessing risks and the information related thereto, retain the relevant study, update it on an ongoing basis, and provide it to the concerned authorities upon request.
2. Financial Institutions, DNFBPs, and Virtual Asset Service Providers shall mitigate the crime risks identified pursuant to Clause (1) of this Article, taking into account the risk-based approach, the results of the National Risk Assessment, and sectoral assessments, and shall comply with the following:

- a. Establish internal policies, controls, and procedures approved by Senior Management, enabling them to manage and mitigate the identified risks, and review and update them on an ongoing basis.
 - b. Ensure that such internal policies, controls, and procedures are proportionate to the nature and size of their business, and monitor their implementation, assess their effectiveness, and enhance them where necessary, in accordance with Article (21) of this Resolution.
 - c. Apply Enhanced Due Diligence measures for the management and mitigation of identified risks, including, by way of example:
 - 1) Obtaining and verifying additional information, such as information on the Customer's identity and occupation, the Beneficial Owner, the amount of funds, and information available through public databases and open sources;
 - 2) Obtaining additional information on the purpose of the Business Relationship or the reasons for expected Transactions or Transactions that have actually been carried out;
 - 3) Updating Customer Due Diligence information on the Customer and the Beneficial Owner more regularly;
 - 4) Taking Reasonable Measures to identify the source of funds and wealth of the Customer and the Beneficial Owner;
 - 5) Increasing the degree and level of ongoing monitoring of the Business Relationship to determine whether it appears unusual or suspicious, and selecting Transaction patterns requiring further scrutiny and review;
 - 6) Carrying out the first payment through an account in the Customer's name held with a Financial Institution subject to equivalent Due Diligence standards;
 - 7) Obtaining approval from Senior Management to commence or continue the Business Relationship with the Customer.
3. Financial Institutions, DNFBPs, and Virtual Asset Service Providers may, upon fulfilling the requirements set out in Clauses (1) and (2) of this Article, and in coordination with the Supervisory Authority, apply Simplified Due Diligence measures to manage crime risks where low risks are identified, unless there is a suspicion that a crime has been committed.

Such Simplified Due Diligence measures shall be proportionate to the elements of low risk and shall ensure full implementation of the instructions issued by the Executive Office or other Competent Authorities in relation to Targeted Financial Sanctions, and may include, by way of example, the following:

- a. Verifying the identity of the Customer and the Beneficial Owner after the commencement of the Business Relationship;
 - b. Updating Customer data at longer intervals;
 - c. Reducing the frequency of ongoing monitoring and Transaction scrutiny;
 - d. Inferring the purpose and nature of the Business Relationship from the type of Transaction or the Business Relationship established, without the need to collect information or undertake specific procedures.
4. Where high risks related to Proliferation Financing are identified, Financial Institutions, DNFBPs, and Virtual Asset Service Providers shall take proportionate measures to manage and mitigate such risks. This includes, by way of example, the following:
- a. Adopting enhanced internal controls aimed at detecting and preventing potential violations of, non-implementation of, or circumvention of instructions of the Executive Office or other relevant Competent Authorities relating to Targeted Financial Sanctions, and conducting ongoing enhanced scrutiny of the Business Relationship to ensure full compliance;
 - b. Maintaining documented records of the measures taken and making them available to the competent authorities upon request;
 - c. Conducting periodic reviews of internal controls in line with changes in the level of risk.

Division Three

Customer Due Diligence and Beneficial Owner Identification Procedures

Article (6)

1. Financial Institutions, DNFBPs, and Virtual Asset Service Providers shall verify the identity of the Customer and the Beneficial Owner before or during the establishment of a Business Relationship or the opening of an account, or prior to carrying out a Transaction for a Customer with whom no such relationship exists.
2. In cases of low crime risk, Financial Institutions, DNFBPs, and Virtual Asset Service Providers may defer the completion of Customer identity verification until after the establishment of the Business Relationship, subject to the following conditions:
 - a. Verification shall be completed as soon as possible after the commencement of the Business Relationship or execution of the Transaction;
 - b. The deferral shall be necessary so as not to disrupt the normal course of business;
 - c. Appropriate and effective measures shall be applied to control the risks of the Crime.
3. Financial Institutions, DNFBPs, and Virtual Asset Service Providers shall take measures to manage risks in circumstances where the Customer is able to benefit from the Business Relationship prior to the completion of the verification process.

Article (7)

1. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers, as applicable, shall apply Customer Due Diligence measures in the following cases:
 - a. Upon the commencement of a Business Relationship;
 - b. Where there is suspicion of a Crime;
 - c. Where there are doubts as to the accuracy or adequacy of Customer identification data previously obtained.
2. Financial Institutions shall apply Customer Due Diligence measures in the following cases:
 - a. When conducting occasional Transactions for a Customer amounting to or exceeding fifty-five thousand dirhams (AED 55,000), whether carried out as a single Transaction or several Transactions that appear to be linked;

- b. When conducting occasional Transactions in the form of Wire Transfers amounting to or exceeding three thousand five hundred dirhams (AED 3,500).
3. Virtual Asset Service Providers shall apply Customer Due Diligence measures when conducting occasional Transactions amounting to or exceeding three thousand five hundred dirhams (AED 3,500), whether carried out as a single Transaction or several Transactions that appear to be linked.

Article (8)

Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall apply Customer Due Diligence measures and conduct ongoing monitoring in respect of the Business Relationship, which shall include the following:

1. Scrutinizing Transactions carried out throughout the duration of the Business Relationship to ensure that such Transactions are consistent with the information available thereto regarding the Customer, the nature of their activities, and the risks they represent, including, where necessary, the source of funds.
2. Ensuring that documents, data, or information obtained as part of Customer Due Diligence measures are up to date and relevant, through reviewing records, with particular emphasis on records relating to categories of High-Risk Customers.

Article (9)

1. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall identify the Customer, whether permanent or occasional, and determine whether the Customer is a natural person, Legal Person, or Legal Arrangement, and shall verify such identity using original documents, data, or information obtained from a reliable and independent source, as follows:
 - a. In respect of Customers who are natural person, obtaining the name as stated in the identity card or travel document, nationality, address, date and place of birth, and, where applicable, the name and address of the employer, together with a true copy of a valid identity card or travel document;

- b. In respect of Customers who are Legal Persons or Legal Arrangements, obtaining the following basic information:
- 1) Name, legal form, memorandum of association, tax registration number of the Legal Persons subject to corporate tax, and the unique reference number, if any;
 - 2) Address of the registered office or principal place of business, and where the Person is foreign, the name and address of its legal representative in the State, if any, together with supporting evidence;
 - 3) Articles of association or any other equivalent approved documents;
 - 4) Names of relevant persons holding Senior Management positions within the Legal Person or Legal Arrangement.
2. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall verify that any person acting on behalf of the Customer is duly authorized to do so, and shall identify such person in accordance with Clause (1) of this Article.
3. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall understand the purpose and the intended nature of the Business Relationship and obtain information relating thereto where necessary.
4. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall understand the nature of the Customer's business and the ownership and control structure thereof.

Article (10)

Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall take into account the risks of the Crime arising from the Customer and the Business Relationship, identify the Beneficial Owner of Legal Persons and Legal Arrangements, and take Reasonable Measures to verify such identity using documents, data, or information obtained from a reliable and independent source, in a manner that enables them to be satisfied that the Beneficial Owner's identity has been determined, as follows:

1. Customers that are Legal Person:

- a. Obtaining the identity of the natural person who ultimately owns, whether individually or jointly with another person, an actual controlling ownership interest or shares in the Legal Person of 25% (twenty-five percent) or more;
 - b. Where there is doubt as to the identification of the natural person under paragraph (a) of this Clause, or doubt that the natural person who owns an ownership interest or controlling shares is the Beneficial Owner, or where no natural person exercises control through ownership interest, the identity of the natural person who exercises legal or actual control over the Legal Person , or through any other means, whether directly or indirectly, shall be identified;
 - c. Where no natural person is identified pursuant to paragraphs (a) and (b) of this Clause, identifying the relevant natural person holding a Senior Management position shall be identified, whether one or more persons.
2. Customers that are Legal Arrangement:
- a. Identifying the identity of the Trustee, Settlor, Trust Protector, Beneficiaries, or classes of Beneficiaries, and the powers and authorities granted thereto where no Beneficiaries are identifiable at the time of establishment of the Trust;
 - b. Identifying the identity of any other natural person exercising ultimate effective control, including through a chain of ownership or control over the trust, whether directly or indirectly;
 - c. Obtaining adequate information regarding the Beneficial Owner to enable the identification thereof at the time of payment or when the Beneficial Owner intends to exercise legally acquired rights;
 - d. Identifying the natural persons holding equivalent or similar positions in other Legal Arrangements;
 - e. Identifying the Beneficial Owner of a Legal Person where such Legal Person is a party to the Legal Arrangement, in accordance with the provisions of this Article.

Article (11)

Where the Customer, or the controlling owner, is a company listed on a securities market that is subject to disclosure requirements ensuring sufficient transparency with respect to the identification of the Beneficial Owner, or a subsidiary thereof holding a controlling interest, it shall be permissible not to identify or verify the identity of any shareholder or Beneficial Owner of such Companies. In such cases, identity information may be obtained from publicly available registers, from the Customer, or from any other reliable sources.

Article (12)

1. In addition to the Due Diligence measures required in respect of the Customer and the Beneficial Owner, Financial Institutions shall apply Due Diligence and ongoing monitoring measures with respect to the beneficiary of life insurance policies and other types of investment-related insurance classes, as soon as the beneficiary is identified or designated, as follows:
 - a. Where the beneficiary is designated by name, name of the person shall be obtained, whether the person is a natural person, a Legal Person, or a Legal Arrangement.
 - b. Where the beneficiary is designated by category or description, such as by family relationship (including spouse or children) or by other means such as a will or estate, sufficient information about the beneficiary shall be obtained to ensure that the Financial Institution will be able to identify the beneficiary at the time of payment of compensation or entitlements.
 - c. In all cases, the identity of the beneficiary shall be verified at the time of payment of compensation or entitlements, or upon the exercise of any rights related to such policies.
2. In all cases, Financial Institutions shall consider the beneficiary of life insurance policies as a risk factor when determining the applicability of Enhanced Customer Due Diligence measures. Where it is determined that such beneficiary is a Legal Person or Legal Arrangement that presents high risk, Financial Institutions shall apply Enhanced Customer Due Diligence measures, which shall include reasonable procedures to identify and verify

the Beneficial Owner of the beneficiary of the insurance policy at the time of payment of compensation or entitlements, or upon the exercise of any rights related to such policies.

Article (13)

Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall apply Customer Due Diligence measures to Customers and existing Business Relationships at the time this Resolution enters into force, at such times as they deem appropriate based on materiality and risk, and shall ensure the adequacy of data previously obtained where Due Diligence measures were applied prior to the entry into force of this Resolution.

Article (14)

1. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall be prohibited from establishing or continuing a Business Relationship or executing a Transaction where they are unable to apply Customer Due Diligence measures, and shall consider submitting a Suspicious Transaction Report to the Unit whenever necessary.
2. Where Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers suspect the commission of a Crime, they may refrain from applying Customer Due Diligence measures if they have reasonable grounds to believe that such measures may result in alerting the Customer, and shall submit a Suspicious Transaction Report to the Unit, stating the reasons for not applying such measures.

Article (15)

Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall comply with the following:

1. Refraining from dealing with Shell Banks in any manner whatsoever, including opening bank accounts therefor or accepting funds or deposits therefrom.
2. Refraining from opening or maintaining anonymous accounts or accounts held under obviously fictitious names.

Division Four
Politically Exposed Persons
Article (16)

1. In addition to applying Customer Due Diligence measures, Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall comply with the following:
 - a. In respect of foreign Politically Exposed Persons:
 - 1) Establishing appropriate risk management systems to determine whether the Customer or the Beneficial Owner is a Politically Exposed Person;
 - 2) Obtaining approval from Senior Management prior to establishing or continuing a Business Relationship with existing Customers who are Politically Exposed Persons.
 - 3) Taking Reasonable Measures to identify the source of funds and wealth of Customers and Beneficial Owners identified as Politically Exposed Persons.
 - 4) Conducting enhanced ongoing monitoring of the Business Relationship.
 - b. In respect of domestic Politically Exposed Persons and persons entrusted with a prominent function in an international organization:
 - 1) Taking adequate measures to determine whether the Customer or the Beneficial Owner falls within these categories.
 - 2) Applying the measures set out in subparagraphs (2), (3), and (4) of paragraph (a) of this Clause where a high-risk Business Relationship exists with such persons.
2. Subject to Clause (1) of this Article, Financial Institutions concerned with life insurance policies shall take Reasonable Measures to determine whether the beneficiary or the Beneficial Owner thereof is a Politically Exposed Person prior to the payment of compensation or entitlements or the exercise of any related rights. Where higher risks are identified, they shall inform Senior Management prior to the payment of compensation or entitlements or the exercise of any related rights, conduct enhanced scrutiny of the entire Business Relationship, and consider submitting a Suspicious Transaction Report to the Unit whenever necessary.

Division Five
Suspicious Transaction Reports

Article (17)

Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall establish indicators through which they are able to identify suspicion of a Crime for the purpose of submitting Suspicious Transaction Reports, and shall update such indicators on an ongoing basis in line with the development and diversification of methods used in the commission of a Crime, in compliance with instructions issued by the Supervisory Authority in this regard.

Article (18)

1. Where Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers suspect, or have reasonable grounds to suspect, that a Transaction or attempted Transaction, or funds, in whole or in part, constitute proceeds, are related to the Crime, or are intended to be used therein, regardless of their value, they shall, without invoking banking secrecy, professional secrecy, or contractual liability, comply with the following:
 - a. Immediately and without delay notify the Unit by submitting Suspicious Transaction Reports, containing all available data and information relating to such Transaction or funds, and related parties, through the Unit's electronic system or any other means approved thereby.
 - b. Promptly respond to any request from the Unit for additional information.
2. Lawyers, notaries, other independent legal professionals, and independent statutory auditors shall be exempt from the provisions of Clause (1) of this Article where the information relating to such transactions was obtained in the course of assessing a Customer's legal position, defending, or representing the Customer before courts, or in arbitration or mediation proceedings, or providing a legal opinion relating to judicial proceedings, including providing advice on initiating or avoiding such proceedings, whether the information was obtained before, during, or after such proceedings, or in other circumstances subject to professional secrecy.

Article (19)

1. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers, as well as their directors, officers, and employees shall be prohibited from disclosing, whether directly or indirectly, to the Customer or any other person that they have submitted or are about to submit a Suspicious Transaction Report, or any information or data related thereto, or that an investigation is being conducted in respect thereof, without prejudice to information sharing with branches and subsidiaries at the level of the Financial Group, in accordance with the provisions of Article (32) of this Resolution.
2. Attempts by lawyers, notaries, other independent legal professionals, or independent statutory auditors to dissuade a Customer from committing an unlawful act shall not constitute disclosure.

Division Six

Reliance on a Third Party

Article (20)

1. Taking into account the countries identified by the National Committee as high-risk and countries with deficiencies in their anti-money laundering, combating terrorist financing, and proliferation financing systems, and to the maximum extent possible the available information on country risks, Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers may rely on a third party to apply Customer Due Diligence measures for the purposes of identifying the Customer and Beneficial Owner and understanding the nature of the Customer's business or for the purposes of a Business Relationship, provided that they remain responsible for the accuracy of such measures and comply with the following:
 - a. Ensuring that the third party is regulated and supervised and complies with Customer Due Diligence and record-keeping requirements pursuant to this Resolution.
 - b. Immediately obtaining from the third party the necessary identification data and information collected during Customer Due Diligence measures, and taking the

necessary steps to ensure the ability to obtain copies of the necessary documents without delay upon request.

2. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers that rely on a third party that forms part of the same Financial Group, shall ensure the following:
 - a. That the Group applies Due Diligence requirements in respect of customers and Politically Exposed Persons, maintains records, and implements anti-crime programs in accordance with Divisions Three, Four, and Eleven of Part One of this Chapter and Article (32) of this Resolution, and that the group is subject, in this regard, to supervision by the competent authority.
 - b. That any high risks related to countries are adequately mitigated through the Group's anti-crime policies and controls.
3. Reliance on a third party shall not include the use by Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers of external sources, such as outsourcing or agency services to perform Customer Due Diligence measures on their behalf, where such services are carried out in accordance with their internal policies and procedures, and the external sources are subject to their supervision and control in the effective implementation of those policies and procedures, and apply fitness and propriety standards and effective audit procedures to their staff.

Division Seven

Internal Supervision and Foreign Branches and Subsidiaries

Article (21)

Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall have internal anti-crime policies, controls, and procedures approved by Senior Management, proportionate to the identified Crime risks and to the nature and size of their activities, and the mitigation thereof. Such policies, controls, and procedures shall be reviewed and updated thereby on an ongoing basis, and shall include the following:

1. Customer Due Diligence measures as required pursuant to this Resolution, including risk management procedures for Business Relationships prior to the completion of the verification process.
2. Procedures for reporting Suspicious Transactions.
3. Appropriate anti-crime compliance management arrangements, including the appointment of a Compliance Officer at management level.
4. Screening procedures to ensure the application of high standards of fitness and propriety in the appointment of employees;
5. Preparation of anti-crime periodic programs and workshops to build the capacities and qualify those assuming the compliance function and other relevant employees.
6. An independent audit function to test the effectiveness and adequacy of internal anti-crime policies, controls, and procedures.

Division Eight

Duties of the Compliance Officer

Article (22)

Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall appoint a Compliance Officer at management level and under their responsibility, who shall have independence in decision-making and possess appropriate competence and experience, and who shall undertake the following duties:

1. Monitoring Transactions related to the Crime.
2. Reviewing records and receiving, examining, and assessing Suspicious Transaction data, and deciding whether to notify the Unit or to retain the matter stating the reasons therefor, in full confidentiality.
3. Reviewing Anti-Money Laundering, and combating Financing of Terrorism, and Proliferation Financing internal systems and procedures, assessing their consistency with the provisions of the Decree by Law and this Resolution, evaluating the establishment's level of compliance with their implementation, proposing what is necessary to update and develop them; and preparing periodic reports thereon to be submitted directly to Senior

Management, and sending a copy thereof to the concerned Supervisory Authority upon its request, including Senior Management observations and decisions.

4. Developing, implementing, and documenting ongoing programs and training plans for employees of the establishment regarding all matters related to the Crime and methods of combating it.
5. Cooperating with the Supervisory Authority and the Unit, providing them with any data they may request, and enabling their assigned personnel to access the records and documents necessary for the exercise of their competencies.

Division Nine

High-Risk Countries

Article (23)

1. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall apply Enhanced Customer Due Diligence measures proportionate to the level of risk arising from a Business Relationship or Transactions with a natural or legal person from countries identified by the National Committee as high-risk, or from countries with deficiencies in Anti-Money Laundering, and combating Financing of Terrorism, and Proliferation Financing systems.
2. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall apply countermeasures and any other measures required by the Supervisory Authority, whether on its own initiative or as determined by the National Committee, in relation to high-risk countries and countries with deficiencies in Anti-Money Laundering, combating the Financing of Terrorism, Proliferation Financing systems.

Division Ten
Requirements Relating to New Technologies

Article (24)

1. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall identify and assess the risks of Money Laundering, Financing of Terrorism, and Proliferation Financing that may arise from the development of new products and new business practices, including new service delivery mechanisms and the use of new or developing technologies for both new and pre-existing products.
2. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall assess such risks prior to the launch or use of products, practices, or technologies, and shall take appropriate measures to manage and mitigate those risks.

Division Eleven
Record-Keeping

Article (25)

1. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall retain all records, documents, instruments, and data relating to all domestic and international financial and cash Transactions and commercial dealings, for a period of not less than five (5) years from the date of completion of the Transaction or the termination of the Business Relationship with the Customer. Such records shall be made available to the concerned authorities promptly upon request.
2. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall retain all records and documents obtained through Customer Due Diligence measures, ongoing monitoring, account files, business correspondence, copies of personal identification documents, including Suspicious Transaction Reports, results of any analysis conducted, closed-circuit television (CCTV) and the related automated teller machines (ATMs) recordings, and any other recordings, for a period of not less than five (5) years from the date of termination of the Business Relationship, or

from the date of account closure for Customers holding accounts therewith, or after the completion of an occasional Transaction, or from the date of completion of inspection by the Supervisory Authority, or from the date of completion of an investigation, or from the date of issuance of a final court judgment, with the retention period calculated by reference to the most recent of such procedures.

3. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall organize retained records, documents, and instruments in a manner sufficient to permit the reconstruction of individual Transactions, data analysis, and the tracing of financial transactions, so as to be capable, where necessary, of providing evidence for prosecution of criminal activity.
4. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall make all Customer information, including information relating to Customer Due Diligence, ongoing monitoring, and the results thereof, as well as records, files, documents, correspondence, and related forms, available to the concerned authorities promptly upon request.

Part Two

Obligations Specific to Financial Institutions

Division One

Correspondent Banking Relationship

Article (26)

1. Prior to entering into a Correspondent Banking Relationship or any other similar relationship, Financial Institutions shall take the following measures:
 - a. Refraining from entering into or continuing a Correspondent Banking Relationship with Shell Banks, or with any institution that permits its accounts to be used by Shell Banks.
 - b. Collecting sufficient information on any respondent Correspondent Institution for the purpose of identifying it and reaching a full understanding of the nature of its business, and, through publicly available information, determining its reputation and the level

- of supervision to which it is subject, including whether it has been subject to an investigation relating to the Crime or to a supervisory action.
- c. Assessing the anti-crime controls applied by the respondent institution.
 - d. Obtaining approval from Senior Management prior to establishing a new Correspondent Banking Relationship.
 - e. Understanding the anti-crime responsibilities of each institution.
2. With respect to Payable-Through Accounts, the Financial Institution shall ensure that the respondent institution has applied Due Diligence measures in respect of Customers who have direct access to such accounts, and that it is able to provide relevant Customer Due Diligence information upon request by the correspondent institution.

Division Two

Money or Value Transfer Services (MVTs)

Article (27)

1. Money or Value Transfer Service Providers shall be licensed by or registered with, the concerned Supervisory Authority. The Supervisory Authority shall take the necessary measures to penalize any person providing such services without the license or registration, in accordance with its applicable legislation, and shall ensure that licensed or registered providers comply with anti-crime controls.
2. Money or Value Transfer Service Providers shall maintain an updated list of their agents and make it available to the concerned authorities within the State in which the Money or Value Transfer Service Providers and their agents operate. They shall also include such agents in the anti-crime programs, and monitor their compliance with such programs.

Division Three

Wire Transfers

Article (28)

1. Financial Institutions shall verify the accuracy of originator information in all international Wire Transfers equal to or exceeding the amount of three thousand five hundred dirhams (AED 3,500), and shall ensure that such transfers are always accompanied by the following data:
 - a. The full name of the originator and the beneficiary.
 - b. The account number of the originator and the beneficiary, or, where no account number exists, the transfer shall include a unique transaction reference number that enables the Financial Institutions to trace it.
 - c. The address of the originator, or the originator's identity number or travel document number, or the date and place of birth, or the customer identification number held by the originating Financial Institution, which shall refer to a record containing such data.
2. Where multiple international Wire Transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the transfer file shall include accurate originator data and complete beneficiary information, which is fully traceable in the beneficiary country, and the Financial Institution shall be required to include the originator's account number or a unique transaction reference number.
3. Financial Institutions shall ensure that all international Wire Transfers below the amount of three thousand five hundred dirhams (AED 3,500) are accompanied by the data referred to in Clause (1) of this Article, without the need to verify the accuracy of such data, unless there are suspicions of the commission of the Crime.
4. Financial Institutions originating domestic Wire Transfers shall ensure that the information accompanying such transfers includes the same originator data specified in Clause (1) of this Article, unless such data is otherwise available to the Beneficiary Financial Institutions and the concerned authorities through other means.
5. Where the information accompanying a domestic Wire Transfer is available to the Beneficiary Financial Institutions and the concerned authorities through other means, the originating Financial Institution shall be required to include only the account number or

the unique transaction reference number, provided that such number permits tracing of the transaction to the originator or the beneficiary. The originating Financial Institution shall provide such data within three (3) Working Days from the date of receipt of a request from the Beneficiary Financial Institution or the concerned authorities.

6. Financial Institutions shall be prohibited from executing Wire Transfers where they fail to comply with the conditions set out in this Article.
7. Originating Financial Institutions shall retain all information collected regarding the originator and the beneficiary in accordance with the provisions of Article (25) of this Resolution.
8. Financial Institutions shall, when processing Wire Transfers, apply freezing measures and transaction prohibition measures in accordance with instructions issued by the Executive Office or other competent authorities relating to Targeted Financial Sanctions.

Article (29)

1. Intermediary Financial Institutions shall ensure that all originator and beneficiary information accompanies international Wire Transfers.
2. Where technical limitations prevent the originator and beneficiary information from remaining with an international Wire Transfer when such transfer is converted into a domestic Wire Transfer, the Intermediary Financial Institution receiving the international transfer shall retain a record containing all information received from the originating Financial Institution or from a foreign intermediary institution, in accordance with the provisions of Article (25) of this Resolution.
3. Intermediary Financial Institutions shall take reasonable and immediate measures to identify international Wire Transfers lacking required originator or beneficiary information, and shall establish risk-based policies and procedures to determine whether to execute, suspend, or reject such transfers, as well as the appropriate follow-up actions in respect thereof.

Article (30)

1. Beneficiary Financial Institutions shall take Reasonable Measures to identify international Wire Transfers lacking required originator or beneficiary information, such as monitoring them during execution, where feasible, or after execution.
2. Beneficiary Financial Institutions shall verify the identity of the beneficiary of international Wire Transfers equal to or exceeding three thousand five hundred dirhams (AED 3,500), where such identity has not been previously verified.
3. Beneficiary Financial Institutions shall establish risk-based policies and procedures to determine when to execute, reject, or suspend Wire Transfers lacking the required originator or beneficiary information, and to determine the appropriate follow-up actions.
4. Beneficiary Financial Institutions shall retain all information collected in respect of the originator and the beneficiary in accordance with the provisions of Article (25) of this Resolution.

Article (31)

1. Money or Value Transfer Service Providers shall comply with all relevant requirements set out in Articles (28), (29), and (30) of this Resolution, whether they conduct their activities directly or through their agents.
2. Where a Money or Value Transfer Service Provider acts as both the originator from the State and the recipient in another State, it shall:
 - a. Collect all information relating to the originator and the beneficiary for the purpose of determining whether to submit a Suspicious Transaction Report;
 - b. Where it is decided to submit a Suspicious Transaction Report in relation to the Transaction, it shall be submitted to the Financial Intelligence Unit of the concerned State, together with all relevant information.

Division Four
Financial Groups

Article (32)

Financial Groups shall implement group-wide programs for combating Crime, which shall be applicable to all branches and subsidiaries in which the group holds a majority ownership. Such programs shall, in addition to what is stipulated in Article (21) of this Resolution, include the following:

1. Policies and procedures for the exchange of information required for Customer Due Diligence and crime risk management purposes;
2. Provision of information relating to customers, accounts, and transactions from branches and subsidiaries to compliance, audit, and Anti-Money Laundering, combating Terrorism Financing officers at the financial group level where necessary for the purposes of combating Crime, including information resulting from the analysis of Transaction, or activities that appear unusual or suspicious, Suspicious Transaction Reports, or information indicating that such a report has been submitted. In all cases, such information shall be made available to branches and subsidiaries where appropriate and where consistent and proportionate with risk management;
3. The provision of adequate safeguards relating to confidentiality, non-tipping-off or notification, and the use of exchanged information.

Article (33)

1. Financial Institutions shall ensure that their foreign branches and subsidiaries, in which they hold a majority interest, apply combating Crime measures in a manner consistent with the requirements of the Decree by Law and this Resolution, where the minimum requirements for combating Crime in the other country are less stringent than those applied in the State, to the extent permitted by the laws and regulations of the other State.
2. Where the other State does not permit the appropriate implementation of combating Crime measures consistent with the requirements of the Decree by Law and this Resolution, Financial Institutions shall take additional measures to manage and mitigate the risks of Money Laundering, Financing of Terrorism, and Proliferation Financing

associated with their foreign operations, shall notify the Supervisory Authority in the State thereof, and shall comply with the instructions issued thereby in this regard.

Part Three

Obligations Specific to Non-Profit Organizations

Article (34)

1. Non-Profit Organizations shall, in coordination with the concerned Supervisory Authority, undertake the following:
 - a. Apply focused, proportionate, and risk-based measures approved by the concerned Supervisory Authority;
 - b. Apply best practices approved by the concerned Supervisory Authority to address vulnerabilities, in a manner that enables them to protect themselves against misuse for the Financing of Terrorism;
 - c. Establish clear policies to enhance accountability, transparency, integrity, and public confidence in their activities and management;
 - d. Conduct Transactions through regulated financial channels whenever possible, taking into account differences in financial sector capacities in various countries and the risks associated with the use of cash, in accordance with applicable legislation in the State.
2. The obligations set out in Clause (1) of this Article shall apply to persons acting on behalf of, or for the benefit of, Non-Profit Organizations.

Part Four

Obligations Specific to the Supervisory Authority of Virtual Asset Service

Providers

Article (35)

1. The Supervisory Authority responsible for Virtual Asset Service Providers may issue decisions, circulars, and procedures necessary for the adequate regulation thereof, and for determining the scope, limits, and form of Virtual Asset Transfers, verification obligations taking into account the level of risks, record-keeping requirements, and necessary

technical standards, in a manner that ensures compliance with the provisions of the Decree by Law and this Resolution.

2. The Supervisory Authority of Virtual Asset Service Providers shall, on its own initiative or in coordination with the concerned authorities, take the necessary measures to identify any person conducting Virtual Asset Service Provider activities without a license, registration, or listing, and to apply appropriate sanctions against them. Such measures may include:
 - a. Reviewing public databases and open sources to identify relevant online advertisements or potential business solicitations made by any person who is not licensed, listed, or registered;
 - b. Establishing feedback channels with the concerned authorities or communication channels to receive public feedback in this regard;
 - c. Coordinating with the Unit to obtain relevant information available thereto;
 - d. Reviewing non-public information, such as information relating to the refusal, suspension, restriction, or revocation of licenses, listing, or registrations, and any other relevant information held by law enforcement authorities.

Part Five

Obligations Specific to Virtual Asset Service Providers and the Scope of Their Application to Financial Institutions

Article (36)

1. Any natural or legal person conducting any Virtual Asset Service Provider activity, offering related products or services, or performing its transactions from within the State shall be licensed, registered, or listed, as applicable, by the competent Supervisory Authority.
2. Virtual Asset Service Providers shall comply with the provisions of Articles (26) to (33) of this Resolution in a manner proportionate to the nature of their activities and in accordance with Supervisory Authority instructions, subject to the following:
 - a. The originating Virtual Asset Service Provider shall obtain and retain accurate originator and beneficiary information of the transfer and shall transmit such information immediately and securely to the beneficiary Virtual Asset Service Provider

or Beneficiary Financial Institution, if any, and shall make such information available to concerned authorities upon request, including such information as determined by the Supervisory Authority and, at a minimum, the following:

- 1) With respect to the originator: name, account number, or Virtual Asset wallet address, and residential or business address;
 - 2) With respect to the beneficiary: name and account number or Virtual Asset wallet address.
- b. The beneficiary Virtual Asset Service Provider shall obtain and retain accurate information on the originator and the beneficiary of the transfer and make it available to concerned authorities upon request.
3. Virtual Asset Service Providers shall comply with all obligations applicable to Financial Institutions set out in the legislation in force in the State relating to Targeted Financial Sanctions.
 4. All requirements set out in Clauses (1) and (2) of this Article shall apply to Financial Institutions where they send or receive Virtual Asset Transfers on behalf of a Customer.

Chapter Three

Transparency and Beneficial Ownership

Part One

Obligations of the Registrar, Companies, Nominee Directors, and Nominee Shareholders

Article (37)

1. The Registrar shall be responsible for registering all Companies and for providing information relating thereto and making such information publicly available, as follows:
 - a. A description of their various types or forms and their basic characteristics;
 - b. Procedures for their establishment;
 - c. Procedures for registration and for obtaining their Basic Information as referred to in Paragraph (b) of Clause (1) of Article (9) of this Resolution;
 - d. Procedures for registration and for obtaining Beneficial Owner information.

2. The Registrar shall obtain and retain the Up-To-Date Basic Information referred to in Paragraph (b) of Clause (1) of Article (9) of this Resolution, together with the Up- to-Date Information of the Nominee Director or Nominee Shareholder referred to in Article (39) of this Resolution, verify the accuracy thereof, make it publicly available, and establish the necessary mechanisms for that purpose.
3. Upon registering Companies, the Registrar shall obtain the company's Beneficial Owner information in accordance with Clause (1) of Article (10) of this Resolution and shall, upon obtaining such information and in all cases, ensure that such information is adequate, accurate, and Up-To-Date, make it available to the concerned authorities, and establish the necessary mechanisms for that purpose.
4. To ensure access to accurate and Up-To-Date Information identifying the Beneficial Owner, the Registrar shall take supplementary measures, such as coordination with competent authorities that retain such information or have access thereto. The Registrar may notify the Supervisory Authority to impose the prescribed administrative sanctions on Companies, or take any other measures it deems appropriate, where it is unable to obtain Beneficial Owner information or where it has doubts as to its accuracy.
5. The Registrar shall coordinate with the Supervisory Authority and the National Committee to identify and assess Crime risks relating to all Legal Persons in the State, take appropriate measures to manage and mitigate such risks, and determine the measures required to ensure that the concerned authorities obtain adequate, accurate, and Up-To-Date Beneficial Owner Information.

Article (38)

1. Companies shall be required to obtain and retain the following:
 - a. The Basic Information referred to in Paragraph (b) of Clause (1) of Article (9) of this Resolution, together with the Up-To-Date information of the Nominee Director or Nominee Shareholder referred to in Article (39) of this Resolution, and shall update such information within fifteen (15) Working Days from the occurrence of any amendment or change thereto, verify their accuracy on an ongoing basis, and assist the Registrar in documenting such information where necessary;

- b. The data of the partners' or shareholders' register, including the number of shares or ownership interests held by each, and the classes of shares, if any, including the nature of the voting rights attached thereto, provided that such data is retained within the State at the company's office, registered place of business, or another location notified to the Registrar;
 - c. The shareholders' register shall be exempt from being retained within the State where the company retains Beneficial Owner information within the State at its office, registered place of business, or at any other location notified to the Registrar, provided that the company shall comply with providing such information to the Registrar upon request and without delay;
 - d. The Beneficial Owner information referred to in Clause (1) of Article (10) of this Resolution, and shall update such information within fifteen (15) Working Days from the occurrence of any amendment or change thereto and verify its accuracy on an ongoing basis.
 2. Companies shall cooperate with Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers in providing adequate, accurate, and Up-To-Date Beneficial Owner Information.
 3. Companies shall cooperate to the maximum extent possible, with the concerned authorities in identifying and making available adequate, accurate, and Up-To-Date Beneficial Owner Information without delay.
 4. No company established and registered in the State may issue bearer shares, bearer share warrants, or any similar instruments that cannot be traced. Bearer shares or bearer share warrants issued prior to the entry into force of this Resolution shall be converted into registered shares in accordance with the legislation in force in the State within thirty (30) Working Days from the date of publication of this Resolution. The holder of bearer shares, bearer share warrants, or similar instruments shall notify the company of their capacity and status, and the company shall register the holder's identity prior to the exercise of any rights attached thereto during the conversion period.

Article (39)

Subject to the legislation in force in the State, and for the purposes of preventing and mitigating Crime risks, a Nominee Director or Nominee Shareholder shall notify the company of their capacity, disclose thereto the information relating to their status and the identity of the person they represent or the Nominator, and notify the company of any change thereto within a period not exceeding fifteen (15) Working Days from the date of such change.

Article (40)

The Registrar, Companies, persons responsible for their management or liquidation, and any other persons concerned with the dissolution of a company, shall retain the records and all information referred to in Articles (37), (38), and (39) of this Resolution for a period of not less than five (5) years from the date of the company's dissolution or cessation of its existence, or from the date on which the company ceases to be a customer of a Financial Institution or professional intermediary.

Part Two

Obligations Relating to Legal Arrangements

Article (41)

1. The competent authorities responsible for regulating Legal Arrangements shall have mechanisms available to:
 - a. Identify the various types, forms, and essential characteristics of Legal Arrangements;
 - b. Determine and describe procedures for establishing Legal Arrangements and for obtaining basic information and Beneficial Owner information in accordance with Paragraph (b) of Clause (1) of Article (9) and Clause (2) of Article (10) of this Resolution;
 - c. Make the information referred to in Paragraphs (a) and (b) of this Clause accessible to all, without delay and in an effective manner;
 - d. Access the Beneficial Owner information relating to Legal Arrangements, Trustees, and their Funds;

- e. Ensure that information relating to Legal Arrangements, including that referred to in Clause (2) of this Article, is Adequate, Accurate, and Up-to-Date.
2. Subject to the risk-based approach, Trustees of Trusts and persons holding a similar or equivalent position in any other Legal Arrangement established or managed in the State, shall:
 - a. Obtain and retain Adequate, Accurate, and Up-to-Date Information on the Beneficial Owner in accordance with Clause (2) of Article (10) of this Resolution;
 - b. Where the parties to the Legal Arrangement are legal persons or other Legal Arrangements, obtain adequate, accurate, and up-to-date basic information and Beneficial Owner information in accordance with Paragraph (b) of Clause (1) of Article (9) and Article (10) of this Resolution;
 - c. Retain basic information relating to supervised intermediaries and service providers, including investment advisers, managers, accountants, and tax advisers.
3. Trustees in Legal Arrangements and persons holding a similar or equivalent position shall maintain the information referred to in Clause (2) of this Article accurately, update it within fifteen (15) Working Days of any amendment or change, and retain such information for a period of not less than five (5) years from the date their dealings with the Legal Arrangement end.
4. Trustees in Legal Arrangements and persons holding a similar or equivalent position shall:
 - a. Disclose their status to Financial Institutions, DNFBPs, and Virtual Asset Service Providers when establishing a Business Relationship or carrying out an Occasional Transaction exceeding the prescribed threshold under this Resolution;
 - b. Cooperate to the fullest extent possible with Concerned Authorities by providing necessary information relating to Legal Arrangements upon request and without delay;
 - c. Provide Financial Institutions, DNFBPs, and Virtual Asset Service Providers, upon request, with information relating to the Beneficial Owner of the Legal Arrangement and the Funds held or managed under the terms of the Business Relationship.
5. Except for Trustees and persons holding a similar or equivalent position, and based on risk, context, and materiality, the Concerned Authorities may obtain, without delay, adequate,

accurate, and up-to-date basic information and Beneficial Owner information relating to Legal Arrangements, their Funds, and Trustees, from any of the following sources:

- a. Competent authorities responsible for regulating Legal Arrangements, or those required under applicable legislation in the State to retain or collect such information, or to establish access mechanisms thereto;
 - b. Financial Institutions, DNFBPs, and Virtual Asset Service Providers;
 - c. Supervised intermediaries and service providers, including investment advisers and managers, accountants, and tax advisers;
 - d. Any other source retaining such information.
6. The Concerned Authorities, in particular Law Enforcement Authorities and the Unit, may request and obtain, without delay, information from Trustees, persons holding a similar or equivalent position, Financial Institutions, DNFBPs, Virtual Asset Service Providers, and any other entity, concerning:
- a. Basic information and Beneficial Owner information of Legal Arrangements;
 - b. The residence of the Trustee or persons holding a similar or equivalent position;
 - c. Funds held or managed by Financial Institutions, DNFBPs, or Virtual Asset Service Providers in relation to Trustees or authorized persons holding a similar or equivalent position with whom they have a Business Relationship or for whom they conduct an Occasional Transaction.
7. The provisions of this Resolution shall apply to all Legal Arrangements established in the State and to foreign Legal Arrangements, regardless of their designation, such as Trusts, fiduciary arrangements, trust contracts or arrangements, endowments, or custodial arrangements, where such foreign Legal Arrangements are connected to or conduct business in the State, or where the Trustees or persons holding a similar or equivalent position reside in the State.

Part Three

Prohibition of Invoking Bank or Professional Secrecy, or Contractual Liability

Article (42)

Banking secrecy, professional secrecy, or contractual liability may not be invoked to prevent the application of the provisions of the Decree by Law and this Resolution in the following cases:

1. Exchange of information between Financial Institutions, where such exchange relates to reliance on third parties, correspondent banking relationships, or Wire Transfers regulated under Articles (20), (26), and (28) to (31) of this Resolution;
2. Exchange of information between Concerned Authorities at the national or international level relating to anti-crime matters.

Part Four

Access to Information

Article (43)

1. The Concerned Authorities, in particular the Public Prosecution, Law Enforcement Authorities, and the Unit, shall obtain, as swiftly and effectively as possible, the basic information referred to in Paragraph (b) of Clause (1) of Article (9) and the Beneficial Owner information referred to in Clause (1) of Article (10) of this Resolution, as held by competent authorities, Financial Institutions, DNFBCs, and Virtual Asset Service Providers.
2. The Concerned Authorities shall, in the context of public procurement, have timely access to the basic information referred to in Paragraph (b) of Clause (1) of Article (9) and the Beneficial Owner information referred to in Clause (1) of Article (10) of this Resolution.
3. The Concerned Authorities shall establish appropriate mechanisms to exchange, or facilitate timely access to, adequate, accurate, and up-to-date Beneficial Owner Information referred to in Clause (1) of Article (10) of this Resolution, in relation to all types of Companies, including foreign Companies and other entities that pose Crime-related risks and whose activities are connected to the State, such as permanent establishments, branches, or agencies, or that maintain substantial commercial activities

or ongoing Business Relationships with Financial Institutions or DNFBPs, or that hold significant real estate or other investments in the State, or are registered for tax purposes therein.

Chapter Four

The Financial Intelligence Unit and the National Committee

Part One

Independence of the Unit

Article (44)

1. The Unit shall operate as the national center for receiving Suspicious Transaction reports and other information relating to the Crime, analyzing such information, and disseminating the results of such analysis to Law Enforcement Authorities.
2. The Unit shall enjoy operational independence, including the authority to decide on the analysis, request, re-dissemination, and referral of information, and shall operate independently with Concerned Authorities and counterpart units in order to perform its functions effectively. No staff member of the Unit may be summoned in relation to their duties without the approval of the Chief of the Unit.
3. The headquarters of the Unit shall be located in the capital of the State, and it may establish sub-branches within or outside the branches of the Central Bank.
4. The Chief of the Unit shall be appointed and removed from office by a decision of the Board of Directors of the Central Bank.
5. For the purpose of performing its duties and competences under the Decree by Law and this Resolution, the Unit shall appoint such qualified and experienced personnel as it deems appropriate and shall determine their duties. The Central Bank shall provide the Unit with the human, financial, and technical resources necessary to enable it to perform its functions effectively.

Part Two
Competences of the Unit

Article (45)

The Unit shall have the following competences:

1. Establishing its organizational structure and internal regulations, which shall include procedures to ensure the efficiency and integrity of its staff, to define their responsibilities in handling sensitive and confidential information, and to prevent access or disclosure of information, except by authorized persons;
2. Establishing a database or special register for the information available thereto, and protecting such information through information security and confidentiality controls, including cybersecurity measures and procedures for processing, storing, and disseminating information, as well as procedures to ensure restricted access to its premises, information, and technological systems;
3. Ensuring that its staff obtain the necessary security clearances and are aware of their responsibilities in handling and disseminating sensitive and confidential information;
4. Providing training courses and programs for the training and qualification of its staff and any other entity, whether within or outside the State;
5. Preparing studies, research, and statistics relating to the Crime, and following up on any national or international studies, research, or statistics prepared in this regard;
6. Preparing annual reports on its anti-crime activities, including, in particular, a general analysis of notifications and Suspicious Transaction reports received by the Unit, Crime activities and trends, and preparing a summary of such reports for publication purposes.

Article (46)

In carrying out its functions in relation to Suspicious Transaction reports, the Unit shall have the following competences:

1. Receive reports from Financial Institutions, DNFBPs, and Virtual Asset Service Providers in accordance with the forms approved by the Unit, examine, analyze, and retain such reports in its database;

2. Request Financial Institutions, DNFBPs, Virtual Asset Service Providers, and Concerned Authorities to provide any additional information or documents relating to the reports and information received by the Unit, as well as any other information it deems necessary for the performance of its functions, including information relating to disclosure systems, customs information, tax information, Population Register information, and the information referred to in Paragraph (b) of Clause (1) of Article (9) and Article (10) of this Resolution, within the timeframes and in the manner determined by the Unit;
3. Analyze reports and available information as follows:
 - a. Operational analysis, using available and obtainable information to identify specific targets such as persons, funds, or criminal networks, trace the course of specific activities or Transactions, and identify links between such targets, activities, or Transactions and potential criminal property;
 - b. Strategic analysis using available and obtainable information, including data provided by the Concerned Authorities, to identify Crime trends and patterns;
4. Provide Financial Institutions, DNFBPs, and Virtual Asset Service Providers with feedback on reports received by the Unit to enhance the effectiveness of Crime combating measures and the detection and reporting of Suspicious Transactions;
5. Cooperate and coordinate with the Supervisory Authority by referring the results of its analyses relating to the quality of reports received, in order to ensure compliance by Financial Institutions, DNFBPs, and Virtual Asset Service Providers with Crime combating procedures;
6. Use dedicated, secure, and protected channels to disseminate report-related data, analysis results, and other relevant information to Law Enforcement Authorities, where sufficient grounds exist to suspect a link to the Crime, for the purpose of taking the necessary actions in this regard;
7. Use dedicated, secure, and protected channels to provide the Public Prosecution and Law Enforcement Authorities with information relating to Crime, including information obtained from Financial Intelligence Units in other countries, whether spontaneously or upon request.

Article (47)

For the purpose of performing its functions at the international level, the Unit shall have the following competences:

1. Exchanging information, both spontaneously and upon request, with counterpart units, regardless of differences in their nature, and with other foreign competent authorities responsible for the suspension or cessation of Transactions suspected of being related to Crime; cooperating in relation to such Transactions, Suspicious Transaction reports, or any other information that the Unit is authorized to obtain or access, directly or indirectly; and exchanging information with Concerned Authorities in the State to facilitate such cooperation.
2. Concluding Memoranda of Understanding to regulate cooperation and the exchange of information with counterpart units and Concerned Authorities, in accordance with the legislation in force in the State.
3. Notifying counterpart units of the results of the use of the information provided and of the analyses conducted on the basis thereof. Such information, including the information referred to in Clause (1) of this Article, shall be used solely for the purposes of combating Crime, and shall not be disclosed to any third party without the consent of the Unit.
4. Following up on developments relating to Crime through relevant regional and international organizations and bodies, and participating in meetings related thereto.
5. Following the requirements of the Egmont Group and attending and participating in its meetings as a member thereof.

Part Three

Competences of the National Committee

Article (48)

The competences of the National Committee shall be expanded to include the following:

1. Identifying, assessing, and understanding Crime risks at the national level, including risks arising from the development of new products or new business practices, such as the use of new or emerging technologies or services or products delivery methods.

2. Updating the National Risk Assessment and the National Anti-Crime Strategy at least once every three (3) years, or whenever necessary.
3. Disseminating information relating to the National Risk Assessment, in accordance with the mechanism it deems appropriate, to Concerned Authorities, Financial Institutions, DNFBPs, Virtual Asset Service Providers, and Non-Profit Organizations.
4. Coordinating with the Concerned Authorities in the application of the risk-based approach, the allocation of resources, and the implementation of Crime combating or mitigation measures.
5. Coordinating with the Registrar and the Supervisory Authority in identifying and assessing Crime risks relating to all legal persons, including foreign-established Companies and others that pose Crime risks and whose activities or investments are connected to the State, taking appropriate measures to manage and mitigate the identified risks, and determining the measures required to ensure that the Concerned Authorities have access to adequate, accurate, and Up-To-Date Beneficial Owner Information.
6. Identifying and assessing Crime risks relating to Legal Arrangements and taking appropriate measures to manage and mitigate the identified risks, including requiring the submission of Beneficial Owner information to be retained by the competent authorities regulating foreign Legal Arrangements or any other authority responsible for retaining such information, in the following cases:
 - a. Legal Arrangements registered or licensed under the legislation of the State, or administered therein;
 - b. Legal Arrangements administered in the State or whose Trustees reside therein;
 - c. Foreign Legal Arrangements whose activities are connected to the State, including those having substantial and ongoing commercial activities or relationships with Financial Institutions or DNFBPs, significant real estate or other domestic investments, or tax registration in the State.
7. Coordinating with the Concerned authorities to ensure that the application of the provisions of the Decree by Law complies with personal data protection and privacy requirements under the personal data protection and privacy legislation in force in the State.

8. Developing and coordinating capacity-building and training programs for personnel working in the field of Anti-Money Laundering, Combating the Financing of Terrorism, and Proliferation Financing.

Chapter Five

Supervisory Authority

Part One

Supervisory Authority over Financial Institutions, DNFBPs, and Virtual Asset Service Providers

Article (49)

The competences of Supervisory Authorities shall be expanded to include the following:

1. Identifying and assessing Money Laundering, Terrorist Financing, and Proliferation Financing risks that may arise from the development of new products and new professional practices, including new service delivery methods and the use of new or emerging technologies for both new and existing products.
2. Applying a risk-based approach to ensure that Money Laundering, Terrorist Financing, and Proliferation Financing prevention or mitigation measures are proportionate to the identified risks.
3. Implementing identified risk-based and proportionate measures and allocating resources efficiently to mitigate Proliferation Financing risks.
4. Issuing instructions, regulations, and forms relating to Crime combating applicable to entities subject to their supervision, where necessary.
5. Establishing policies, procedures, and controls necessary to verify the compliance of supervised entities with the provisions of the Decree by Law, this Resolution, and any other Crime combating legislation in the State, and requesting information relating to the implementation thereof.
6. Establishing systems, rules, and standards of merit and eligibility, and taking all necessary legal or regulatory measures on an ongoing basis at the time of licensing, registration, renewal, or amendment, to prevent criminals or their associates from holding or being the

Beneficial Owners of significant or controlling interests in Financial Institutions, DNFBPs, or Virtual Asset Service Providers, or from controlling or participating in their management or operation, directly or indirectly.

7. Coordinating with the Unit in identifying indicators of suspected Crime through which Financial Institutions, DNFBPs, and Virtual Asset Service Providers submit Suspicious Transaction reports to the Unit.
8. Coordinating with the Unit regarding the quality of reports and information received by the Unit from Financial Institutions, DNFBPs, and Virtual Asset Service Providers, and taking the necessary supervisory measures in this regard.
9. Conducting off-site and on-site supervision and inspections of Financial Institutions, DNFBPs, and Virtual Asset Service Providers on a risk-based basis, and for that purpose, requesting and obtaining any information deemed necessary for the performance of supervisory functions.
10. Determining the frequency of supervisory and inspection activities over Financial Institutions, DNFBPs, and Virtual Asset Service Providers based on:
 - a. The National Risk Assessment;
 - b. The characteristics of Financial Institutions, Financial Groups, DNFBPs, and Virtual Asset Service Providers, including their diversity, size, and degree of discretion permitted under the risk-based approach;
 - c. Crime risks, the level of understanding thereof, and the internal policies, controls, and procedures applied by Financial Institutions, Financial Groups, DNFBPs, and Virtual Asset Service Providers, as determined in the Supervisory Authority's assessment of the risk structure specific to each of them.
11. Taking all measures necessary to ensure the full and immediate compliance of Financial Institutions, DNFBPs, and Virtual Asset Service Providers with instructions issued by the Executive Office or other competent authorities regarding Targeted Financial Sanctions, through on-site visits and continuous follow-up, and imposing effective, proportionate, and dissuasive administrative penalties in cases of violation or failure to comply.
12. Verifying that supervised institutions adopt and implement the prescribed controls, procedures, and measures under the Decree by Law and this Resolution, and apply them

to their foreign branches and majority-owned subsidiaries to the extent permitted by the laws of the host country.

13. Ensuring that Financial Groups apply appropriate additional measures to manage Money Laundering and Terrorist Financing risks where the laws of the host country do not permit proper implementation of the prescribed controls, procedures, and measures. Where such additional measures are insufficient, the Supervisory Authority shall take supervisory measures, including imposing further controls on the Financial Group or requiring the closure of its operations in that country.
14. Ensuring that Financial Institutions subject to International Core Principles for Financial Supervision are regulated and supervised in accordance with those principles, including the application of consolidated supervision at the Financial Group level for AML/CFT purposes, and ensuring that other Financial Institutions are subject to regulation, supervision, or monitoring commensurate with their Money Laundering or Terrorist Financing risk.
15. Reviewing the institution's and the Financial Group's Crime risk structure assessment, including compliance risks, periodically or upon material developments in the management or operation thereof.
16. Establishing adequate controls and procedures to ensure that Financial Institutions, DNFBPs, and Virtual Asset Service Providers are notified of and comply with National Committee decisions relating to:
 - a. Enhanced Due Diligence measures and countermeasures determined by the National Committee;
 - b. Any concerns relating to deficiencies in AML/CFT/CPF systems in other countries;
 - c. Any other decisions issued by the National Committee.
17. Providing supervised entities with instructions, guidance, and feedback to assist in implementing national Crime combating measures, particularly in detecting and reporting Suspicious Transactions and applying Simplified Due Diligence measures where low risks are identified, to enhance the effectiveness of Crime combating implementation.

18. Maintaining an updated list of Compliance Officers of supervised entities, notifying the Unit thereof, and requiring such entities to obtain its prior approval before appointing their Compliance Officers.
19. Organizing awareness programs and campaigns relating to Crime combating.

Part Two

Supervisory Authority over Non-Profit Organizations

Article (50)

The Supervisory Authority for Non-Profit Organizations shall have the following competences:

1. Obtaining available information from all competent authorities regarding the activities of Non-Profit Organizations from reliable sources in a timely manner, for the purpose of determining their size, characteristics, and types, assessing risks to identify the nature of Terrorist Financing risks to which they are exposed, identifying the sub-sector thereof most exposed to such risks, and establishing focused, proportionate, and risk-based measures to address them, in a manner consistent with the risk-based approach, and periodically reviewing such measures to ensure their adequacy.
2. Supervising and monitoring Non-Profit Organizations using focused, proportionate, and risk-based measures to prevent their misuse in supporting or financing Terrorism, requiring the implementation of such measures and other obligations, and monitoring compliance therewith.
3. Reviewing the adequacy and sufficiency of legislation relating to Non-Profit Organizations to prevent their misuse in supporting or financing Terrorism, and working to improve such legislation whenever necessary.
4. Periodically assessing Non-Profit Organizations by reviewing Up-to-Date Information on potential vulnerabilities that may render them susceptible to exploitation in supporting or financing Terrorism.
5. Cooperating and coordinating with Non-Profit Organizations to develop best practices for addressing vulnerabilities that enable them to protect themselves from misuse in Terrorism Financing.

6. Encouraging and implementing awareness and education programs to raise awareness among Non-Profit Organizations and donors regarding their potential vulnerabilities, which expose them to the risk of misuse in the field of supporting and financing Terrorism, and of measures that can be taken to protect themselves from such risks.
7. Cooperating, coordinating, and exchanging information at the national level with all Concerned Authorities that retain relevant information relating to Non-Profit Organizations.
8. Establishing adequate controls and procedures to ensure that Non-Profit Organizations are notified of, and implement, the relevant decisions of the National Committee.
9. Possessing detection expertise and the capacity to examine Non-Profit Organizations suspected of being exploited by terrorist activities or organizations, or of supporting them.
10. Obtaining full access, during detection and examination processes, to information relating to the management and organization of any Non-Profit Organization, including financial information and information relating to its programs.
11. Conducting off-site and on-site inspections of Non-Profit Organizations without obstructing or delaying their legitimate charitable activities.
12. Establishing mechanisms to ensure the immediate exchange of information with Concerned Authorities for the purpose of taking preventive or investigative measures where there are suspicion or reasonable grounds to suspect that a Non-Profit Organization:
 - a. Is a front for fundraising by a terrorist organization, or is being misused to finance Terrorism.
 - b. Is being exploited as a conduit for Terrorism Financing, for evading funds-freezing measures, or for any other form of terrorist support.
 - c. Conceals or obscures the trail of funds intended for legitimate purposes, but redirected for the benefit of terrorists or terrorist organizations.
13. Identifying appropriate points of contact and the necessary procedures for responding to international requests for information relating to Non-Profit Organizations suspected of engaging in, or being exploited for, Terrorism Financing or the support thereof.

Chapter Six
Provisional Measures and Investigation Procedures

Part One

Provisional Measures

Article (51)

1. The Chief of the Unit may order the suspension or cessation of a Transaction suspected of being related to the Crime, immediately and without prior notice, for a period not exceeding ten (10) working days, based on the Unit's analysis of Suspicious Transaction reports, information, or requests received from domestic or international sources, including counterpart Units regardless of their nature, or any authorities competent to take such measures.
2. The Unit shall establish a system governing the controls and procedures for the suspension or cessation of suspicious Transactions related to the Crime and the circumstances under which such suspension or cessation is lifted upon revocation of the order or expiry of the prescribed period.
3. The Chief of the Unit may order the freezing of funds suspected of being linked to a Crime held by Financial Institutions, DNFBPs, or Virtual Asset Service Providers, without prior notice, for a period of thirty (30) days, based on the Unit's analysis of Suspicious Transaction reports and other information received thereby.
4. Where the decision referred to in Clause (3) of this Article is taken, the Unit shall:
 - a. Notify the relevant Financial Institutions, DNFBPs, or Virtual Asset Service Providers to implement the freezing order, without prior notice;
 - b. Notify the Attorney General or their delegate of the freezing decision and the grounds for suspicion, who may amend or revoke the decision or issue any directions deemed appropriate.
5. A freezing order may be extended by the Attorney General or their delegate for such period they determine upon the Unit's request, stating the justifications therefor.

6. The Chief of the Unit shall submit a proposal to the Attorney General to cancel the extension of the freezing order where the grounds therefore cease to exist, for such action as they deem appropriate.
7. Financial Institutions, DNFBPs, and Virtual Asset Service Providers holding frozen funds shall notify the owner of the frozen funds of the freezing order and its issuing authority, request them to provide the documents necessary to prove the integrity of the Transaction and the legitimacy of the source of funds, and refer the same to the Unit to take the appropriate actions.
8. Financial Institutions, DNFBPs, and Virtual Asset Service Providers shall lift the freezing order where it is revoked by the Chief of the Unit, or where the period specified in Clause (3) of this Article expires without extension.

Article (52)

1. The Public Prosecution and the competent court, as the case may be, may order, without prior notice, the identification, tracing, valuation, seizure, or freezing of Criminal Funds or Property, or Funds of equivalent value, the prohibition of their management, and the imposition of travel bans until the conclusion of the investigation or trial.
2. Where necessary, the Public Prosecution and the competent court, as the case may be, may order travel bans and take decisions preventing dealings in or disposition of Criminal Funds or property or funds of equivalent value, and take the necessary measures to prevent any disposition intended to evade seizure, freezing, or confiscation orders, without prejudice to the rights of bona fide third parties.
3. Without prejudice to the rights of bona fide third parties, any contract or disposition entered into with the accused shall be null and void by operation of law where the parties thereto, or any of them, knew, or ought to have known, that its purpose was to affect the ability of competent authorities to seize, freeze, recover, or confiscate, or to enforce such measures.
4. For the purposes of Clause (3) of this Article, knowledge of the contracting parties with the accused shall be inferred from the factual and objective circumstances surrounding the conclusion of the contract or disposition.

Article (53)

1. The Public Prosecution and the competent court, as the case may be, may:
 - a. Assign the accused, the owner, holder, or manager of Funds, or any other person deemed appropriate, to estimate and manage Criminal Funds or Property, or funds of equivalent value, that have been seized, frozen, subject to confiscation, or subject to Asset Recovery pursuant to an international judicial cooperation request, determine the scope of management and disposal powers in accordance with the legislation in force in the State, provided that the person assigned to manage and dispose shall demonstrate competence, integrity, and absence of conflicts of interest, and submit periodic reports on the managed Funds, including their status, expenses, and returns, if any, and if necessary, the mechanism for their disposition. The assignee may be removed where mismanagement or breach of the limits of their powers is established;
 - b. Authorize the disposal or sale of Criminal Funds or Property, or any funds of equivalent value, even prior to the issuance of a judgment, where necessary, such as where there is a risk of deterioration or loss of economic value over time, or where management or safeguarding costs exceed their value upon sale, or where they are subject to total or partial deterioration. The proceeds from such sale shall accrue to the public treasury upon issuance of a final confiscation judgment.
2. Criminal Funds or Property, or funds of equivalent value, shall remain encumbered, within the limits of their value, by any compensation, rights, or obligations lawfully determined in favor of the victim or any bona fide third parties.
3. Subject to the legislation in force in the State, the General Attorney shall form a committee to assess management fees and expenses of Funds, determine its rules of procedures, composition, and conditions for exercising its competences in determining such fees and expenses, when the management is assigned to a third party. The Committee shall also determine the method of payment, either as a lump sum or a percentage not exceeding (10%) ten percent of the value of the managed Funds. For the purposes of exercising its competences, the Committee may seek assistance from experts as it deems appropriate from governmental or non-governmental entities, taking into account the type, value, and complexity of the Funds under management, any return generated, and the efforts exerted

in management. The fees and expenses shall be deducted from the managed Funds pursuant to a decision approved by the Attorney General.

Article (54)

1. Orders to freeze Funds held by Financial Institutions, DNFBPs, or Virtual Asset Service Providers shall be executed solely by the competent Supervisory Authority or the Unit, as the case may be.
2. Financial Institutions and Virtual Asset Service Providers shall transfer frozen Funds to interest-bearing or profit-generating deposit accounts at prevailing market rates where such freezing is pursuant to decisions issued by competent authorities.
3. Interest and profits accruing from frozen Funds shall be deemed an integral part of the Criminal Property where a confiscation judgment is issued.
4. Frozen Funds, together with accrued interest and profits, shall be returned where the freezing order is lifted by competent authorities.
5. Financial Institutions, DNFBPs, and Virtual Asset Service Providers shall not dispose of seized or frozen Funds under any circumstances, including for the settlement of prior obligations, unless coordination is effected with the competent Supervisory Authority to obtain authorization from the Public Prosecution or the competent court, as the case may be.
6. Without prejudice to the legislation in force in the State, seizure or freezing orders issued by the competent authorities shall not prevent the enforcement of administrative fines imposed by the Supervisory Authority prior to the issuance of the order. This shall be carried out by requesting the release of an amount equivalent to the value of the imposed administrative fines from the scope of the order, at the discretion of the competent authorities.

Part Two
Investigation Procedures

Article (55)

1. The Public Prosecution, on its own initiative or at the request of Law Enforcement Authorities, where sufficient indications of a Crime exist, may order the search of persons and premises, prohibit suspects from travel, obtain evidence, identify, trace, and seize Funds, monitor accounts, intercept communications, directly access accounts, registers, instruments, and documents held by third parties, access computer systems and information technology means, examine correspondence, communications, and parcels, conduct controlled deliveries, and take any other measures that assist in the detection of the Crime and its perpetrators, without prejudice to the legislation in force in the State.
2. The Public Prosecution may seek the opinion of the Unit on the financial aspects of the Crime and their analysis, and request all information available thereto.
3. Law Enforcement Authorities shall receive and follow up on the Unit's reports, collect intelligence and information relating thereto, and provide feedback to the Unit regarding actions taken in connection therewith.
4. The Public Prosecution and Law Enforcement Authorities may access, in a timely manner, without delay and without prior notice, any information deemed necessary for the prompt identification and tracing of Criminal Funds or Property, or Funds of equivalent value, or any other information as they deem necessary, even if such information is subject to banking or professional secrecy, where required for the performance of their duties for the detection of the Crime or its perpetrators. Where necessary, they shall conduct parallel financial investigations, by undertaking the following:
 - a. Taking into account the extent of linkage of the financial aspects of the Crime, in order to determine its temporal and geographic scope, the value of Criminal Property and the manner of its acquisition, to identify, trace, and seize such property or Funds of equivalent value, that may be subject to confiscation, identify the person to whom the Criminal Property has been transferred and their relationship with the accused, their disposal thereof, and their knowledge of its source; to strengthen the evidence proving the commission of the Crime and attributing it to its perpetrator; to demonstrate their

- financial capacity before and after the criminal activity and the extent of its proportionality to their legitimate sources of income, and take all precautionary measures in preparation for legal confiscation;
- b. Coordinating with Concerned Authorities, each within its competence, to obtain timely access to any information and documents relating to the Crime, including disclosure systems, customs, tax, Population Register, property registers, and bank account records and those managing them, and other information deemed necessary for the performance of their duties;
 - c. In all cases, Law Enforcement Authorities shall, immediately upon becoming aware of the Crime, promptly identify, trace, and seize the Criminal Funds or Property, or Funds of equivalent value, potentially subject to confiscation.
5. Law Enforcement Authorities may collect witness statements, conduct undercover operations and other intelligence-gathering activities, use various detection methods, and carry out controlled deliveries where such measures would lead to the detection of the Crime and its evidence, identification of the source and destination of Criminal Property, or arrest of perpetrators, without prejudice to the legislation in force in the State.

Chapter Seven

National Cooperation and Coordination

Article (56)

1. Concerned Authorities shall cooperate and exchange expertise and information among themselves, including tax information, to enhance efforts for Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing, particularly with respect to asset recovery and identification of Criminal Property.
2. Concerned authorities may enhance and develop partnerships with the private sector to exchange expertise and facilitate access to information in the field of Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing.

Chapter Eight
International Cooperation and Asset Recovery
Part One
General Provisions on International Cooperation
Article (57)

In applying the provisions of this Chapter, due regard shall be given to the legislation in force in the State and the provisions of treaties or agreements to which the State is a party, or the principle of reciprocity.

Article (58)

For the purpose of requesting and executing international cooperation requests relating to the Crime, the Concerned Authorities shall:

1. Provide the widest possible range of international cooperation promptly, constructively, and effectively, and exchange information spontaneously and upon request.
2. Establish clear procedures for prioritizing and executing incoming international cooperation requests in a timely manner.
3. Cooperate, coordinate, and exchange information among themselves to enhance the effectiveness of Asset Recovery at the international level.
4. Conclude, negotiate, and sign agreements and other mechanisms with competent foreign authorities in a timely manner.
5. Participate in multilateral networks to facilitate prompt and constructive international cooperation in the field of Asset Recovery.
6. Consider applying for membership in inter-agency or inter-authority networks supporting international cooperation in the field of Asset Recovery.
7. Take the necessary measures to enable informal cooperation with other countries for Asset Recovery purposes, including facilitating assistance prior to the submission of formal requests, updating requesting countries on the status of their requests, and providing assistance based on initial requests without the need for supplementary requests, where appropriate.

8. Request additional information from competent foreign authorities where necessary to execute or facilitate the execution of international cooperation requests.
9. Request information on behalf of foreign counterpart authorities, obtain any other required information on their behalf, and exchange all obtainable information as if the request had been made at the national level.

Article (59)

The Concerned Authorities shall give priority to all international cooperation requests, particularly those relating to the Crime, and shall execute them urgently and without undue delay through clear and secure procedures, mechanisms, and channels to enhance information protection, and shall in all cases:

1. Use information obtained through international cooperation solely for the purpose for which it was requested, unless consent is granted by the competent foreign authorities for another purpose.
2. Provide feedback to the competent foreign authorities on the use and benefit of the information obtained, where requested.
3. Maintain the confidentiality of international cooperation requests and the exchange of information with competent foreign authorities in a manner consistent with each party's obligations regarding privacy and data protection, and in accordance with the legislation in force in the State, in order to protect the integrity of the investigation and the request for information relating thereto. Where confidentiality of received information cannot be maintained, the requesting authority shall be notified accordingly.
4. Ensure, where exchanging information with competent foreign authorities, their ability to guarantee the confidentiality of the exchanged information; and Concerned Authorities shall protect the information obtained pursuant to clear procedures and in the same manner in which they protect similar information from domestic sources. The Concerned Authorities may refuse to provide or exchange any information where the competent foreign authorities are unable to protect such information effectively.

Article (60)

1. International cooperation requests shall not be refused or subjected to unreasonable or unjustified conditions that restrict their execution. In all cases, such requests shall not be refused on the grounds of any of the following:
 - a. That the request involves financial, customs, or tax matters, whether direct or indirect;
 - b. Confidentiality requirements applicable to Financial Institutions, DNFBPs, or Virtual Asset Service Providers, except where the information was obtained under circumstances covered by legal professional privilege or professional secrecy;
 - c. That the request is related to a Crime under ongoing detection or judicial prosecution in the State, if the request would impede such proceedings, response may be deferred until completion thereof;
 - d. Differences in the nature or status of the requesting competent foreign authority as compared with the nature or status of the Concerned Authorities in the State.
2. Where execution of an international cooperation request is refused or deferred, Concerned Authorities shall notify the requesting authority of the reasons therefor.
3. Dual criminality shall not be a condition for executing international cooperation requests that do not involve coercive compulsory measures.
4. Where an international cooperation request involves coercive compulsory measures, dual criminality shall be required and deemed satisfied where the act constituting the Crime is punishable under the legislation in force in both the State and the requesting country, regardless of the type, description, or category of the Crime. Where dual criminality is not satisfied, the requested coercive measures may nonetheless be executed with the consent of the person concerned.

Part Two

Exchange of Information Between the Concerned Authorities and Foreign Counterpart and Non-Counterpart Authorities

Article (61)

The Concerned Authorities shall exchange Crime-related information with competent foreign authorities, and in doing so, they may:

1. Exchange information indirectly with non-counterpart foreign authorities, provided that the competent authority requesting the information indirectly shall always clarify, to the authority from which the information is requested, the purpose of the request and the authority on whose behalf the request is made.
2. Obtain an acknowledgment or undertaking from the foreign authorities that the information exchanged through international cooperation shall be used solely for the purpose for which it was requested, unless such authorities obtain prior consent for its use for another purpose.

Article (62)

1. The Concerned Authorities shall exchange information relating to Companies and Legal Arrangements with competent foreign authorities without imposing unjustified restrictive conditions. This cooperation shall include the following:
 - a. Facilitating access by competent foreign authorities to Basic Information and Beneficial Owner information of Companies and Legal Arrangements and other information held by or available in relevant registers;
 - b. Exchanging information on shareholders;
 - c. Exercising their powers to obtain all Beneficial Owner information on behalf of competent foreign authorities.
2. The Concerned Authorities shall oversee the quality of execution of incoming international cooperation relating to requests for Basic Information and Beneficial Owner information of Companies and Legal Arrangements, including requests concerning the identification of a Beneficial Owners resident outside the State.

3. The Concerned Authorities shall retain Basic Information and Beneficial Owner information of Companies and Legal Arrangements in a secure and easily accessible manner.
4. The Concerned Authorities shall designate and make publicly available contact points responsible for exchanging Basic Information and Beneficial Owner information of Companies and Legal Arrangements.

Article (63)

The Supervisory Authority for Financial Institutions shall:

1. Exchange Crime-related information that it holds or has access to, directly or indirectly, with foreign counterpart authorities, regardless of their nature, in accordance with International Core Principles for Financial Supervision, particularly those relating to the exchange of supervisory information relevant to Anti-Money Laundering, Combating the Financing of Terrorism, as applied by each authority.
2. Exchange information for Crime countermeasures purposes with other Supervisory Authorities having shared responsibility over Financial Institutions operating within the same Financial Group, including:
 - a. Regulatory information, such as information relating to the regulatory system and general information on financial sectors;
 - b. Prudential information under the Core Principles, such as information on the Financial Institution activities and operations, their Beneficial Owners, management, and fit and properness;
 - c. Crime countermeasure information, such as internal policies and procedures of Financial Institutions for combating Crime, customer due diligence information, customer files, and samples of accounts and Transaction information.
3. Obtain prior consent from foreign Supervisory Authorities providing information before referring or using such information for supervisory or non-supervisory purposes, and notify them where disclosure results from a legal obligation.
4. Request information on behalf of foreign Supervisory Authorities or facilitate their access to information for the purpose of enhancing supervision over the Financial Group.

Article (64)

1. The Concerned Authorities shall apply the provisions of this Chapter in exchanging information and executing international cooperation requests relating to Crimes involving Virtual Assets and Virtual Asset Service Providers as promptly and comprehensively as possible.
2. The Supervisory Authority over Virtual Asset Service Providers shall exchange information with foreign counterpart authorities, regardless of differences in designation or regulatory status of the counterpart authority or the Virtual Asset Service Providers in other countries.

Article (65)

The Law Enforcement Authorities shall:

1. Exchange information that they hold or have access to, directly or indirectly, including disclosure system and customs information, with foreign counterpart authorities for detection or intelligence-gathering purposes related to a Crime, identification and tracing of Criminal Property or Funds of equivalent value, and support freezing, seizure, and confiscation measures through mutual judicial assistance.
2. Initiate domestic reports based on information received from foreign counterpart authorities, on their own initiative or upon request of the Public Prosecution, and conduct detections and gather intelligence accordingly.
3. Spontaneously exchange information relating to Criminal Property or Funds of equivalent value with foreign counterpart authorities, and identify and trace them within the State where there are grounds to believe they are linked to investigations in another country, without impeding any ongoing domestic detections or investigations in the State.
4. Exercise all legally available powers to conduct investigations, gather intelligence, and provide information, documents, or other evidence in execution of international cooperation requests.
5. Obtain information on behalf of foreign counterpart authorities and coordinate the formation of bilateral or multilateral joint investigation teams to carry out joint detection.

Part Three
International Judicial Cooperation

Article (66)

Competent judicial authorities shall, upon request from judicial authorities of another country with which the State has a valid agreement, or on the basis of reciprocity, promptly, and in a constructive, and effective manner provide judicial assistance in investigations, prosecutions, or proceedings relating to the Crime, and may order:

1. The identification, tracing, evaluation, seizure, freezing, or confiscation of Criminal Funds or Property, or funds of equivalent value. The fact that the accused is unknown, lacks criminal responsibility, or that the criminal proceedings have lapsed shall not prevent the adoption of such measures.
2. Any other investigative measures or methods that may be applied in accordance with the legislation in force in the State, including the provision of records held by Financial Institutions, Designated Non-Financial Businesses and Professions, Virtual Asset Service Providers, or Non-Profit Organizations, the search of persons and premises, the collection of witness statements, evidence gathering, and the use of investigative methods such as covert operations, interception of communications, the collection of electronic data and information, and controlled delivery.
3. The surrender and recovery of persons and Criminal Property expeditiously without undue delay.

Article (67)

International judicial cooperation requests relating to judgments or judicial orders providing for seizure, freezing, or other provisional measures, or confiscation in all its forms of Criminal Property or funds of equivalent value issued by competent courts or judicial authorities of another country may be executed. For the execution of such request, it shall not be required to conduct national investigations, where the request contains sufficient information and facts on which its execution may be based.

Article (68)

Execution of judgments or judicial orders referred to in Article (67) of this Resolution, shall be subject to the condition that it does not conflict with a judgment or order previously issued by a court in the State, and that there is no case pending in the State concerning the same subject matter as that in respect of which the judgment was issued by the requesting country. The request shall include the following documents and information:

1. A certified copy of the confiscation judgment or order, the law upon which it is based, and the statement of the reasons for its issuance where not stated therein;
2. Proof that the convicted person was duly summoned, properly represented, and was enabled to defend themselves;
3. A document confirming that the judgment or order is final and enforceable;
4. A description of the Criminal Property or funds of equivalent value sought to be confiscated, an assessment of their value, their probable location, and information on any person who may be holding or possessing them;
5. A statement of the value of the amount sought to be recovered from the funds subject to confiscation;
6. Any information relating to third-party rights in the criminal property or funds of equivalent value subject to confiscation;
7. A statement of measures taken by the requesting country to protect bona fide third parties.

Article (69)

1. Competent judicial authorities may request judicial assistance from judicial authorities of another country to uncover the Crime, its circumstances, and perpetrators, and to identify, trace, evaluate, freeze, seize, or confiscate Criminal funds or property, or funds of equivalent value, or to recover such funds or property, or to request the recovery of objects or persons.
2. Where the competent judicial authorities of another country requires a judicial order issued by courts of the State for execution of judicial assistance pursuant to Clause (1), the competent court, as the case may be, shall issue such order on its own initiative or upon

request of the Public Prosecution following the approval of the Attorney General or their delegate.

Chapter Nine

Final Provisions

Article (70)

Cabinet Resolution No. (10) of 2019, referred to herein, is hereby repealed, and any provision that contradicts or conflicts with the provisions of this Resolution is also repealed.

Article (71)

This Resolution shall be published in the Official Gazette and shall enter into force thirty (30) days after the date of its publication.

Mohammed bin Rashid Al Maktoum

Prime Minister

Issued by us:

On: 7 Jumada Al-Ula 1447 A.H.

Corresponding to: 29 October 2025 A.D.