Chapter Five: Guidelines for Combating Money Laundering, Counterterrorism Financing, and Funding of illegal Organizations.

Chapter One: Introduction

Article 1: Preamble

This chapter provides mandatory standards for the concerned individual to ensure that the anti-money laundering measures align with the laws and regulations applicable in the country, particularly the federal laws related to combating money laundering. This chapter should be read in conjunction with federal laws on combating money laundering, as well as other relevant laws in the country and any developments in standards and best practices. The individual concerned should consider how these matters mentioned above may impact their day-to-day operations.

Article 2: Objectives of the Chapter

The purpose of this chapter is as follows:

1. To specify the requirements related to the laws and regulatory provisions specific to the federal laws for combating “money laundering” crimes in the country.

2. To provide a foundation for the concerned individual to develop and implement a compliance program for combating money laundering, aiming to prevent and detect money laundering crimes.

3. To emphasize the responsibilities of the Board of Directors and senior management of the concerned individual in preventing and detecting “money laundering” crimes.

4. To provide guidance on the effective application of a risk-based approach.

5. To enhance the use of a proportionate and risk-based approach to due diligence measures and directing resources toward clients most exposed to risk.

6. For the concerned individual to take necessary steps in managing risks associated with violations by criminals and terrorist groups.

7. The concerned individual should be aware that refraining from reporting any suspicious activity related to the federal laws for combating money laundering constitutes a criminal offense.

This chapter should not be considered as an internal guideline., since the concerned individual should develop and apply a compliance program for combating money laundering tailored to the nature of the activity and services provided, risk profiles, and compliance frameworks. This should include risk profiles, compliance frameworks, and taking into consideration the principles and standards outlined in this chapter and federal laws for combating money laundering. Additionally, the individual must ensure the ongoing effectiveness of implementing this program in line with regulatory requirements and expectations.

Article 3: Definitions

Country: United Arab Emirates.

Authority: Securities and Commodities Authority.

Executive Office for Control and Prohibition of Proliferation: The entity responsible for implementing the provisions of Federal Decree-Law No.

43 of 2021 regarding goods subject to proliferation prohibition. This aims to prevent unauthorized and unlawful trading of dual-use goods contributing to the production or development of weapons of mass destruction, associated technologies, and their means of delivery.

Federal Laws for Combating Money Laundering: All federal laws of the United Arab Emirates and related executive regulations addressing money laundering, terrorism financing, funding of unauthorized organizations, and the financing of arms proliferation. This also includes the common guide for combating money laundering and terrorism financing issued by regulatory authorities in the country, available on the Authority's official website.

Money Laundering: Refers to financing terrorism, funding unauthorized organizations, and financing arms proliferation according to the provisions of this chapter.

Compliance Program for Combating Money Laundering: It is a set of policies, systems, and internal controls specific to the concerned individual with the aim of compliance with federal laws for combating money laundering.

Financing Terrorism: Refers to any specific acts defined in Articles 29 and 30 of Federal Law No. 7 of 2014 concerning the combatting of terrorist crimes.

Unauthorized Organizations: Criminal organizations established or engaged in criminal activities.

Facilitating Unauthorized Organizations: Any material act or legal transaction aimed at providing funds to an Unauthorized organization or any of its activities or members.

Money Laundering Crime: 1. Money laundering is committed by anyone who knowingly commits a felony or misdemeanor and intentionally performs any of the following acts:

a. Transfer or move proceeds for the purpose of concealing or disguising the unlawfully obtained funds.

b. Conceal the true nature of the proceeds, their source, location, method of disposal, movement, ownership, or related rights.

c. Acquire, possess, or use the proceeds upon receiving them.

d. Assist the perpetrator of the original crime in escaping punishment.

Money laundering is considered an independent crime, and the punishment of the perpetrator of the original crime does not exempt them from being punished for money laundering.

2. Conviction of the original crime is not required to prove the illegitimate source of the proceeds.

Concerned Individual: Refers to the licensed entity authorized by the Authority to engage in any financial activity specified in the Financial Activities Rulebook, excluding credit rating agencies, and all licensed providers of virtual asset services, whether by the Authority or local entities in the country.

Ultimate Beneficial Owner (UBO): The natural person who holds ultimate ownership or exercises ultimate control over a legal person directly or

indirectly through a chain of ownership, control, or other indirect means. Also, the natural person on whose behalf transactions are conducted or who exercises effective ultimate control over a legal person, as defined according to the regulations issued by the Council of Ministers in 2020 concerning the regulation of procedures for the UBO.

Agent: Anyone who engages or is authorized to engage in any of the activities specified in Article 2 of the Cabinet Resolution No. 24 of 2022 with one of the financial institutions or providers of virtual asset services.

Legal Arrangement: The relationship arising under a contract between two or more parties that does not result in the creation of a legal entity, such as Trust funds or similar arrangements.

Trust Fund: A legal relationship whereby the legator places funds under the control of the trustee for the benefit of a beneficiary or for a specific purpose. The funds remain independent of the trustee ’s ownership, and the right to the funds is in the name of the legator or another person on behalf of the legator.

Trustee:

A natural or legal person endowed with rights and powers granted by the legator or the Trust fund. The legator manages, uses, and disposes of the funds according to the conditions imposed on them by either party.

Legator:

A natural or legal person who entrusts the management of their funds to a trustee under a document.

Due Diligence Measures:

The process of identifying and verifying client or beneficial owner information, whether a natural or legal person or legal arrangement, understanding their nature of business, the purpose of the business relationship, ownership structure, and the control, whether legal, regulatory, or factual, exercised over them.

Enhanced Due Diligence Measures: Refers to the measures mentioned in Article 2 of the third chapter of this section.

Simplified Due Diligence Measures: Refers to the measures outlined in Article 3 of the third chapter of this section.

Suspicious Transaction: Transactions related to funds with reasonable grounds to suspect they are obtained from any criminal offense or felony or are linked to financing terrorism or the funding of unlawful organizations, whether executed by legal provisions or not.

Targeted Financial Sanctions: Asset freezing and other financial measures to prevent the availability of funds or other assets directly or indirectly for individuals, entities, and organizations listed on local and international lists.

Business Relationship: Any continuous business or financial relationship between financial institutions or designated non-financial businesses and professions and their clients, relating to activities or services provided to them.

Financial Group: A collection of financial entities comprising a holding company or another legal entity exercising control over the rest of the group. It coordinates functions to implement control at the group and its

subsidiaries, adhering to international financial control principles, policies, and measures, including anti-money laundering and counter-terrorism financing.

Politically Exposed Persons (PEPs): Natural persons entrusted with or previously entrusted with prominent functions in the State or any other country, such as heads of State or government, high-ranking politicians, senior government officials, judicial or military officials, senior executives of State-owned companies, senior officials of political parties, and the persons have been entrusted or previously been entrusted to manage international organizations or any prominent position therein, This definition extends to:

1. Direct family members of the politically exposed person, spouses, children and their spouses, and parents.
2. Close associates of the politically exposed person:
    - Persons who have joint beneficial ownership of a legal person, legal arrangement, or any close business relationship with the politically exposed person.
    - Persons who have sole beneficial ownership of a legal person or legal arrangement for the benefit of a politically exposed person.

Third Party: The third party shall have an independent employment relationship with the client separate from that with the relevant person relying on the third party. The specific procedures applicable to the third party shall be implemented to carry out the due diligence procedures towards clients.

Outsourcing: The contracting entity with the relevant person within the framework of implementing due diligence procedures on behalf of the relevant person. It effectively oversees the relevant person to ensure compliance with their actions, subject to effective execution and in accordance with the recommendations, particularly those outlined in

Recommendation 17 and its interpretative note from the Financial Action Task Force (FATF).

Originating Transferring Institution: The institution initiating the wire transfer and transferring funds upon the request of the transferor. It is the source of the transfer.

Wire Transfer: A financial transaction conducted by a financial institution itself or through an intermediary, on behalf of a transferor, to convey a monetary amount to a beneficiary in another financial institution, whether the transferor and the beneficiary are the same person or different.

Beneficiary Institution: The financial entity that receives the wire transfer from the financial institution originating the transfer directly or through an intermediary financial institution, allowing funds to be made available to the beneficiary.

Intermediary Institution: The financial entity responsible for receiving and transmitting the wire transfer between the financial institution originating the transfer and the beneficiary financial institution or another intermediary financial institution.

Travel Rule: The term referred to in the recommendations of the Financial Action Task Force (FATF).

Wire Transfer Message File: A transfer composed of individual wire transfer instructions sent to the same financial institution, which may or may not be ultimately directed to different individuals.

Unique Transaction Reference Number for Payment Protocols: A combination of letters, numbers, or symbols determined by the payment service provider according to settlement systems or messaging systems used in wire transfers.

Transferor: The account holder authorizing the wire transfer from their account, or in the absence of an account, the natural or legal person issuing instructions to the financial institution originating the transfer for the execution of the wire transfer.

Reasonable Measures: Actions taken that are proportionate to money laundering risks.

Financing the Proliferation of Weapons: Refers to the danger of collecting, moving, or generating funds and other assets and economic resources, either full or partial funding, for individuals or entities with the goal of spreading weapons of mass destruction. This includes the spread of delivery methods or materials associated with them, including the exploitation of dual-use technology for illicit purposes.

Non-for-profit Organizations (NPOs): Groups with organized structures, whether for a specific or indefinite duration, composed of natural or legal persons or other legal arrangements, not aimed at making a profit. They engage in collecting, receiving, or disbursing funds for charitable, religious, cultural, educational, social, or solidarity purposes or other benevolent purposes.

Article (4) Scope of Application:

The provisions of this chapter apply to all of the following:

1. The relevant person.

2. Members of the board of directors, senior management, and employees of the relevant person.

3. Any other person referred to in this chapter.

Chapter Two: Risk Assessment

Article (1): Application of the Risk-Based Approach

- Annex (1) provides an illustrative diagram of the risk-based approach.

- The relevant person commits to:

1. Adopting a risk-based approach to identify and manage potential risks efficiently and effectively in combating money laundering crimes.

2. Identifying, assessing, and addressing money laundering risks under this chapter through reviewing the risks encountered by the relevant person due to the nature of business, clients, products, services, and any other relevant matters in the context of money laundering. Subsequently, adopting an approach proportional to mitigate those risks.

3. When conducting any assessment, ensuring that the risk-based approach for the purpose of complying with the requirements of this chapter is:

a. Objective and proportionate to the risks.

b. Based on reasonable grounds.

c. Properly documented.

d. Reviewed and updated at appropriate intervals.

Article (2): Business Risk Assessment

Section One: Money Laundering Business Risk Assessment

- Annex (2) illustrates the diagram for assessing money laundering business risks.

1. The relevant person commits to taking appropriate steps to identify and assess money laundering risks that its business may face, considering the nature, size, and complexity of its activities.

2. The relevant person shall consider, when identifying and assessing risks under subsection (1) of this article and to an appropriate extent, weaknesses related to:

a. Types of clients and their activities.

b. Countries or geographic regions in which its business operates.

c. Products, services, and business activity profiles.

d. Channels for delivering or distributing services or products and business partners.

e. The complexity and volume of its transactions.

f. Development of new products, business practices, including delivery mechanisms, new channels, and new business partners.

g. Use of new or advanced technologies for both new and existing products.

3. The relevant person commits to considering its day-to-day operations when taking measures to identify and assess risks under subsection (1) of this article, including:

a. Development of new products and business practices.

b. Acquisition of new clients.

c. Changes in its business profile.

4. The relevant person commits to using the information obtained in assessing its business risks to:

a. Develop a program compliant with combating money laundering and maintain its effectiveness as required in subsection three of this article.

b. Ensure that the compliance program to combat money laundering is sufficient to mitigate risks as part of subsections (1,2,3) of this article.

c. Evaluation of the Effectiveness of the Compliance Program to Combat Money Laundering, as Required in Subsection (3) of this Article.

d.Allocation and Identification of Priorities for Resources to Combat Money Laundering.

e. Customer Risk Assessment.

5. Considering the above, the relevant person commits to taking reasonable measures to ensure the assessment, identification, and understanding of “money laundering” risks associated with products, business practices, or technology. Taking appropriate steps to manage and mitigate those risks before launching or using any of those products, practices, or technology.

Section Two: Compliance Program to Combat Money Laundering

The relevant person commits to the following:

1. Developing a compliance program to combat “money laundering” and ensuring that the compliance program is maintained ,. Ensure compliance with federal laws to combat money laundering.

2. Ensuring that the compliance program to combat “money laundering” referred to in subsection (1) of this article from Section Three meets the following:

a. Includes authorities allowing senior management to obtain information related to the effectiveness and operation of the program, Consistently work to help identify and measure “money laundering” risks in order to appropriately manage these risks.

b. The relevant person can determine whether the client or the ultimate beneficiary is a politically exposed person.

3.The effective evaluation and regular update of the Anti-Money Laundering compliance program to ensure its ongoing continuity and ability to identify, assess, monitor, understand, and manage money laundering risks efficiently and comprehensively according to its complexity.

Article 3: Customer Risk Assessment

First: Customer AML Risk Assessment:*

- Annex (3) illustrates the diagram for assessing customer risks.

- The relevant person commits to:

1. Conduct a risk assessment for each client.

2. Categorize the client's risk according to the specific AML risks associated with each client.

3. Perform client risk assessment as specified in sub-articles 1 and 2 before implementing due diligence measures, especially for new clients and if possible for current clients.

4. Complete the following when conducting the customer risk-based assessment in accordance with subsection (1) of this paragraph :*

a. Identify the client, ownership, control, and ultimate beneficiary, if any.

b. Obtain information about the purpose and nature of the client's business relationship.

c. Obtain information about the client's nature, ownership, control structure, and ultimate beneficiary, in addition to considering the nature of its business and relationship.

d. Consider the client's original country, residence, nationality, or place of incorporation or place of work.

e. Consider the relevant product, service, or transaction related to the client.

f. Consider the results of the business risk assessment.

5. Take into account key risk factors, including:

A. Customer risk factors, including:

1- Indicators suggesting an unconfirmed suspicion in the client's data and ownership.

2- Client residing in a region with high geographical risks according to item (c) of this subsection related to geographic risk factors.

3- The customer is a legal person or legal arrangement being used for holding personal assets.

4. The customer is a company with registered shareholders or bearer shares.

5. The customer is a company with intensive cash usage, such as businesses where the majority of their revenues are in cash.

6. The institutional structure of the customer is unusual or highly complex compared to the nature of the business.

B. Factors of risk for the product, service, transaction, or customer identification mechanisms and service provision, including:

1. The service includes specialized banking services.

2. The product, service, or transaction includes a feature of non-disclosure of identity.

3. Business relationships or transactions that occur indirectly with the client using modern technologies such as electronic signatures.

4. Receipt of payments from unidentified persons or third parties not connected to the client.

5. Utilization of new products or services, including pre-developed mechanisms for customer identification, service provision and new technologies for current products or services.

6. Services that involve providing acting directors (nominee director) or registered shareholder (nominee shareholders), or establishing companies in other countries.

C. Geographic risk factors, including:

1. Specific countries identified in reports and reliable sources, such as mutual evaluations, detailed assessment reports, or follow-up reports issued by the Financial Action Task Force (FATF), the International Monetary Fund (IMF), the Organisation for Economic Co-operation and Development (OECD), and other international organizations that indicate the absence of effective systems to combat money laundering or non-compliance with anti-money laundering requirements consistent with the recommendations of the FATF.
2. Countries identified by reliable sources to have high levels of corruption or other criminal activities, such as terrorism, money laundering, or the production and trafficking of illegal drugs.

3. Countries subject to sanctions, prohibitions, or similar measures issued by the United Nations or a specific country. For example,

countries providing financing or support for terrorism or those classified by a State or other countries as having terrorist organizations operating within their territories.

6.Consideration of the following low-risk factors when evaluating "money laundering" risks:

A. Customer risk factors, including if the customer is:

1. A public Authority or an entity owned by the public sector.

2. A resident client or an entity registered in a geographic area with low risks.

3. A financial institution subject to regulation and supervision by a regulatory Authority applying anti-money laundering regulations equivalent to the standards set forth in the Financial Action Task Force recommendations.

4. A subsidiary company of the aforementioned financial institution in item (3).

5. A publicly listed company, with its securities accepted by the Securities and Commodities Authority or accepted by a regulatory Authority equivalent to it.

B. B. Geographical Risk Factors, including:

1. Specific countries mentioned in reliable reports and sources, such as mutual evaluations, detailed reports, or monitoring reports issued by the Financial Action Task Force (FATF), the International Monetary Fund (IMF), the Organization for Economic Cooperation and Development (OECD), and other international bodies that indicate the presence of effective systems to combat money laundering or the implementation of anti-money laundering requirements in line with the recommendations of the Financial Action Task Force.

2.Countries identified by reliable sources as having low levels of corruption or other criminal activities, such as terrorism, money laundering, or the production and trafficking of illicit drugs.

7. When assessing the low-risk factors referred to in item (6) above, the concerned individual commits to always consider that the presence of one or more risk factors may indicate a specific situation.

Secondly, arrangements preventing the identification of the ultimate beneficiary

the person concerned commits to:

1. Refrain from establishing a business relationship with the client if the legal entity or legal arrangement of the client prohibits the person concerned from identifying one or more of the ultimate beneficiaries.

2. Refrain from establishing or continuing business relationships with dummy banks.

Thirdly: Dummy and Anonymous Accounts

The concerned person commits to refraining from establishing or continuing relationships with anonymous or fictitious accounts, or accounts operated for the benefit of another person, or controlled or operated for the benefit of another person without disclosing their identity, in accordance with federal laws combating money laundering.

Fourthly: Use of Internal Coded or Abbreviated Accounts

The person concerned, when using a coded or abbreviated account for clients, shall ensure the following:

1. That this account will only be used for internal purposes.

2. Implementation of due diligence measures towards clients, as required for account holders of other clients.

3. Retention of the required information for the accounts and other account holders.

4. Ensuring full access for employees responsible for combating money laundering tasks, including employees responsible for identifying and monitoring suspicious transactions, and employees in charge of compliance and auditing, to all information related to the account and the account holder.

Chapter Three: Due Diligence Measures for the Client and Continuous Monitoring

Article 1: Due Diligence Measures

First: Due Diligence Measures for the Client:

- Annex No. (4), the illustrative form of due diligence measures and continuous monitoring, clarifies the following:

1. The concerned person commits to the following:

a. Ensure due diligence measures and continuous monitoring towards each client according to (third) item in this article.

b. **Implementing enhanced due diligence measures** towards clients classified by it as high-risk clients under Article 2 of this chapter.

2. The concerned person may conduct **simplified due diligence** towards clients classified by it as low-risk clients under Article 3 of this chapter.

Second: Timing of Due Diligence for Clients

1. The concerned person commits to the following:

A. When establishing a business relationship with the client, the concerned individual is committed to taking appropriate due diligence measures according to clauses (third/1(A, B, C) of this article.

B. After establishing a business relationship with the client, due diligence measures must be performed according to clause (third/1/(D) of this article.

2. The concerned person is committed to taking appropriate due diligence measures at any time in case of:

- A. Doubts about the accuracy or adequacy of documents, data, or information obtained for the purpose of due diligence towards clients.

- B. Suspicions regarding money laundering related to the client.

- C. Changes in the client's risk classification or any event leading to changes in circumstances, information, or documents related to the client.

2. The concerned individual may establish a business relationship with the client before completing the required verification process fully according to clauses (third/1, 2, 3) of this article, provided that the concerned person commits to:

A. Fulfilling all essential documentary requirements for the client's file, without causing undue disruption to normal business operations.

B. The postponement of verification should be necessary and does not hinder the normal course of work.

C. Managing minimal and related risks, including money laundering and any other risks effectively.

D. Ensuring sufficient safeguards to prevent the closure of the client's financial account and refraining from conducting any financial transactions by or on behalf of the account holder (client) until the verification process is completed.

E. Completing the verification as soon as possible by a maximum of 30days from the beginning of the relationship with the client.

4. In case it is not possible to complete the verification within 30 days, the concerned person commits to end the relationship before the end of 30 days as the following:

- A. Documenting the reason for non-compliance.

- B. Recording the non-compliance in the semi-annual anti-money laundering report.

5. The Authority may determine a suitable timeframe for the required verification process according to item (secondly/3/e) and suspend any business relationship with the client within this framework.

6.The person in question is committed to ensuring that the anti-money laundering compliance program includes policies and procedures for risk management related to the conditions under which business relationships with clients can be established before completing the verification process.

Thirdly: Due Diligence Requirements:

1. The following due diligence measures are required to be implemented:

- a. Client identification and verification.

- b. Identify and verify the identity of the real beneficiary

- c. Take reasonable measures and precautions to understand the nature of the client, their business, ownership, and the structure of control over the client if the client is a legal person or legal arrangement.

D. Ongoing Due Diligence Measures and Continuous Monitoring of the Client:

2. The concerned person commits, in case someone wishes to act on behalf of the client, to take the following measures:

- A. Verify the identity of the person wishing to act on behalf of the client.

- B. To act on behalf of the client, ensure that this person is authorized.

- C. Confirm that this person is not listed in local or international lists related to targeted financial sanctions.

3.The concerned person commits to verifying that the documents, data, and information required for the fulfillment of the previous clauses are authentic and reliable, obtained from independent and trustworthy sources.

4.For the purpose of implementing due diligence measures, the person concerned commits to obtaining client information to identify and verify their identity through a Know Your Business model, including:

A. In the case of a natural person:

1. Legal full name, including any aliases.

2. Residence status, whether residing in the country or not.

3. Legal nationality (for citizens and residents).

4. Permanent address in the country, if applicable.

5. Landline telephone number, if available, and mobile phone number.

6. Email address, if applicable

7. Date of birth.

8. Nationality or nationalities, if applicable.

9. Country of birth.

10. Type of identification, whether it is the UAE identity card, passport, or national identity card of a Gulf Cooperation Council (GCC) country.

11. ID number, place of issue, and expiration date.

12. Occupation.

13. Expected annual turnover, including the anticipated annual value and the number of transactions to be monitored for future transactions.

B. In the case of a legal person:

1. Full legal name of the legal person.

2. Place of incorporation and business location, whether inside or outside the country.

3. Address (P.O. Box, building name and number, street, city, emirate, country).

4. Phone numbers and fax number.

5. Email address.

6. Date of incorporation.

7. Type of identification, whether it is a commercial license or its equivalent.

8. Commercial license number or its equivalent, place and date of issue, and expiration date.

9. Activity of the legal person.

10. Names and details of the identities or licenses of controlling and beneficial persons.

11. Names and details of the identities of senior management of the legal person.

12. Names and details of the identities of persons authorized to conduct transactions on behalf of the legal person.

13. Expected annual turnover, including the anticipated annual value and the number of transactions for future transaction monitoring.

14. The basic system of the legal person or its equivalent in other countries.

C. In case the client is a non-for-profit association:

1. A certified copy of the association's articles of association and internal regulations or any other documents constituting the association.

2. Documentary evidence of the appointment of the trustee or any other person exercising authorities in the association.

D. In case the client is an explicit trust fund or any similar legal arrangement

1. A certified copy of the instrument or other documents specifying the nature of the explicit trust fund or arrangement and its conditions.

2. Documentary evidence of the appointment of the trustee or any other person exercising authorities under the trust fund or legal arrangement.

5. The concerned person commits to identifying the real beneficiary for legal entities, legal arrangements, and other legal agreements and

verifying them using information, data, and documents obtained from a reliable source as follows

A. Clients as legal entities:

1. Obtain the identity of the natural person, whether acting individually or with another person who owns a stake of 25% or more. If this is not possible or there is doubt about the information obtained, their identity shall be determined by any other means.

2. If the person exhausts all possible means and cannot identify the real beneficiary owner, according to the required percentage for the legal entity, or if the controlling shareholder is not the actual beneficiary, the senior management of the legal entity must be treated as the actual beneficiary, subject to the approval of the relevant person's senior management. This is required if there are reasons to suspect "money laundering," whether it is an individual or more.

3. In the application of the preceding paragraph (2) of this item, the concerned person must maintain a written record of all actions taken to identify the real beneficiary in the legal entity.

4. The concerned person may refrain from the procedures outlined in paragraphs (3), (2), (1) above regarding the identification of the real beneficiary in the legal entity, provided that they comply with the procedures in the Common Regulatory Guidance on Knowing the Real Beneficiary, if the client:

.A company listed on a regulated stock market, or a licensed stock market, or a regulatory Authority equivalent to the Authority subject to disclosure requirements through any means imposing sufficient transparency requirements about its operations, structure, and identification of the real beneficiary.

A subsidiary company majority-owned by a parent company or holding company.

In case the client is a non-profit association:

1. Identification of the founder, trustee, contributing donors, eligible beneficiaries, and any other persons entitled to receive any assets or income from the organization, along with any other natural person exercising absolute effective control over the association.

2. Identifying the qualified beneficiaries or other individuals entitled to receive assets or income from the association based on characteristics or category, and obtaining sufficient information to distinguish the recipient's identity, whether they are the eligible beneficiary or any other person, before making any payment or transferring ownership to the recipient.

1. Verifying the identity of the recipient, whether the qualified beneficiary or any other person referred to in the preceding paragraph 2(b), before making any payment or transferring any assets from the association to that recipient.

C. If the client is a trust fund or legal arrangement:

1. Identifying the identity of the trustee, legator, or those holding similar positions, beneficiaries, or categories of beneficiaries, and any other natural person exercising actual ultimate control over the legal arrangements, and obtaining sufficient information about the real beneficiary so that their identity can be determined with them when making the payment or when they intend to exercise their acquired legal rights.

2. For the explicit trust fund, identifying the founder, administrator, trustee, custodian, executor, endorser, and any other natural person exercising effective ultimate control over the trust fund. For

other types of legal arrangements, individuals holding equivalent or similar positions to those referred to above.

3. The concerned person is committed to verifying the identity of the legator before distributing to the beneficiary or before the endorser exercises acquired rights.

D. If the client is a politically exposed person:

1. Taking reasonable measures to determine whether the client or the real beneficiary is a politically exposed person.

2. If the client or the real beneficiary is a politically exposed person:

- A. Obtaining the approval of senior management to initiate or continue the business relationship with the client.

- B. Taking reasonable measures to identify the source of the client's wealth and the source of funds of the real beneficiary.

- C. Undertaking continuous and enhanced monitoring to determine whether the client's transactions or activities appear unusual or suspicious.

Article 2: Enhanced Due Diligence Measures

The concerned party commits, when conducting enhanced due diligence, to:

1. Obtain and verify additional information about:

a. Client's and beneficial owner's information.

b. Nature intended for the business relationship.

c. Information regarding the reasons for the transaction.

2. 2. Regularly update information on the client and beneficial owner in a more systematic manner.

3. Take reasonable measures to identify the source of funds and wealth for the client and beneficial owner.

4. Increase the level and nature of monitoring the business relationship to determine if the client's transactions or activities appear unusual or suspicious.

5. Obtain approval from senior management to initiate a business relationship with the client.
6. Ensure that any initial payment made by the client to open the account is through a bank account in the client's name or through a licensed financial institution subject to federal laws addressing money laundering, exceeding those applicable in the country, and the financial action task force.

Article 3: Simplified Due Diligence Measures

1. The concerned party may conduct simplified due diligence as follows:

a. Periodically update client data as needed.

b. Verify the client's identity by requesting a copy of their identification document.

c. Reduce the rate of continuous monitoring and examination of operations, based on the nature of the transaction.

d. Eliminate the need to gather additional information or perform additional procedures if it is concluded that the purpose and nature of the business relationship do not warrant such actions.

2. The concerned party commits to ensuring that the measures taken in paragraph 1 of this article are proportionate to the client's "money laundering" risks.

Article 4 Continuous Due Diligence and Continuous Monitoring Measures

The concerned person commits to the following when conducting continuous due diligence and continuous monitoring:

1. Reviewing transactions during the period of business engagement to ensure the consistency of operations conducted with available information about clients, their activities, and the risks they pose, including financial resources whenever necessary.

2. Giving special attention to complex or unusually large transactions or unusual transaction patterns based on recognized warning indicators, whether they serve a clear economic or project purpose.

3. Verifying the background of the mentioned transactions in item 2 of this article and its purpose.

4. Regularly updating the sufficiency of due diligence information towards clients held, especially for high-risk clients, in case of any significant changes or events related to the client.

5. Periodically updating the client risk profile when any significant changes or events related to the client occur, ensuring that the client's risk classification remains unchanged.

Article 5 Continuous Monitoring of Targeted Financial Sanctions

The concerned person commits to regularly examining databases and transactions related to their business against the names listed in the sanctions issued by the United Nations Security Council, or the relevant committees, as well as local lists and any other lists adopted by the concerned person based on their specific risk approach.

Article 6 Failure to Perform or Complete Due Diligence Measures

1. In case it becomes impossible to conduct or complete continuous due diligence and continuous monitoring required towards the client, the concerned person commits to taking the following actions:

a. Refraining from conducting any transaction with the client or on their behalf through a bank account or in cash.

b. Not opening an account for the client, establishing a business relationship, providing services, or engaging in transactions indirectly.

c. Terminating or suspending any existing business relationship with the client.

d. Returning any funds or assets received from the client.

e. Investigating and inquiring in case of the necessity to report a suspicious transaction or activity.

2. The concerned person, if suspecting the commission of a crime due to the non-application of due diligence measures towards the client, should, if reasonable grounds exist that applying such measures might alert the client, report the suspicious transaction with a financial intelligence unit of the reasons for not applying those measures.

3.The concerned person commits to not applying due diligence measures towards the client if directed to do so by the regulatory Authority or financial intelligence unit.

Chapter Four: Reliance on a third party and outsourcing

Article (1) Reliance on a third party

1. Appendix No. (5) provides an illustration of reliance on a third party.

2. The concerned person may rely on a third party to conduct customer due diligence measures on its behalf, provided that the third party must be either of the following:

a. An entity licensed by the Authority or a supervisory authority similar to the Authority.

B. A financial institution licensed by the competent authorities in the country or outside it.

C. A law firm, accounting firm, or auditing firm licensed by the competent authorities

in the country and specializes in money laundering procedures.

D. A member of the financial group of the concerned person who is subject to and applies the Money Laundering Law and its bylaw.

3. The concerned person may rely on a third party to conduct customer due diligence measures only, provided that The person fulfills the following:

a. Ensure effective due diligence procedures concerning the third party and the retention of records, including evaluating the comprehensiveness of their policies, procedures, and controls against money laundering, as well as the number of employees involved in providing due diligence measures.

b. Establish a mechanism to review and monitor quality assurance policies related to due diligence procedures, including questionnaires, performance cards, and field visits to assess the commitment of the third party.

c. Verify that the third party complies with the recommendations of the Financial Action Task Force, particularly numbers 10, 11, and 17.

d. Verify their ability to obtain due diligence information from the third party promptly upon request.

e. Ensure that the third party has not obtained any exemptions regarding any due diligence requirements.

f. Confirm that if the third party is located outside the country, it complies with due diligence requirements for clients and maintains records that meet the standards outlined in the Financial Action Task Force recommendations under this section.

g. Subject to compliance with due diligence requirements, ensure that the third party is:
    1. Subject to due diligence requirements for clients and maintains records that meet the standards outlined in the Financial Action Task Force recommendations and this chapter.
    2. subject to similar regulatory oversight by an equivalent regulatory Authority or competent Authority in achieving compliance with regulatory standards outlined in the Financial Action Task Force recommendations.

4.It is permissible if the concerned person relies on a third-party member within the financial group not to implement article (1/3/d) , provided that the member commits to the following:

a. Implementing and executing due diligence measures towards clients at the financial group level, retaining records, politically exposed persons, and anti-money laundering programs that comply with the standards outlined in the Financial Action Task Force recommendations.

b. Ensuring the effectiveness of due diligence measures, record retention, politically exposed persons, and anti-money laundering programs at the financial group level, and confirming their supervision by an equivalent regulatory Authority or competent Authority in the country, in line with the regulatory standards outlined in the Financial Action Task Force recommendations.

5. The concerned person, when evaluating the third party, especially if it is located outside the country or is a member of an international financial group, should take into account the following factors:

a. Mutual evaluation results, assessment reports, or follow-up reports published by the Financial Action Task Force, the International Monetary Fund, the World Bank, or other international organizations.

b. The membership of the State to which the third party belongs in the Financial Action Task Force or other international or regional groups, such as the Middle East and North Africa Financial Action Task Force or the Gulf Cooperation Council.

c. Influencing factors such as political stability or the level of corruption in the other country or regulatory Authority, which can be measured through:

1. Advisory notices from the Financial Action Task Force.

2. General assessments of the anti-money laundering system in the other country or regulatory Authority by organizations referred to in subsection (a).

3. Other relevant specialized non-governmental organizations.

6. When conducting an assessment of the third party under the previous clause of this article, the concerned person must rely on up-to-date sources of information and maintain sufficient records of the assessment process, including the sources and materials used.

7.The concerned person may rely on information previously obtained by the third party for due diligence measures, provided that such information is recent.

8.The concerned person is committed to immediately taking due diligence measures towards the client or the ultimate beneficiary regarding any deficiencies in knowledge or information presumed to be known.

Article 2 Responsibility When Relying on a Third Party

The concerned person is not exempt from bearing the responsibility for compliance, as they are solely responsible in all cases, whether first or last, for any failure or inability to meet the requirements of due diligence towards the client, even when relying on a third party.

Article 3 Reliance on Outsourcing

The concerned person is allowed to outsource the implementation of due diligence procedures of clients to another person on their behalf, whether from within or outside the country, after ensuring the competence of the outsourced tasks, with the necessity to comply with the general outsourcing rules outlined in the financial activity regulations.

Chapter Five: Telegraphic Transfers and Traveler's Cheques

Article 1: The Institution as the Source of the Transfer

1. The concerned person (the institution as the source of the transfer) commits to the following before conducting a telegraphic transfer of funds:
    a. Determine the identity of the transferor and verify it if not possible to know the identity beforehand.
    b. Record the details of the fund transfer including (but not limited to): date of transfer, name of the transferor, name of beneficiary, type and value of the transferred fund and the value of virtual asset at transfer.

2.The concerned person (the institution as the source of the transfer) is committed, in the case of transferring an amount of 3500 dirhams or more, to include payment instructions related to the transfer of funds or telegraphic transfer, , the following information:

a. The name of the transferor
b. The account number of the Transferor (or the reference number for the transaction if an account number is not available).
c. The name of the beneficiary.
d. The account number of the beneficiary (or the reference number for the transaction if an account number is not available).

3.The concerned person (the institution as the source of the transfer) is also committed, in the case of transferring an amount of 3500 dirhams or more, to include the following details in the payment instructions:

a. The address of the Transferor.

b. The national ID number of the Transferor, such as the Emirates ID or passport number.

c. The customer identification number of the Transferor.

d. The date and place of issuance of the Transferor's document.

4.If the aggregation of multiple telegraphic transfers across borders, originating from one conversion entity, is to be transferred to beneficiaries, the responsible person (the transferring institution) must consider the provisions outlined in item 3 and item 2 of this article, and to ensure:

a. that the transfer file includes information about the initiator as outlined in item 3 and item 2

b. Verify the information about the Transferor.

c.Verify that the transfer file includes information about the beneficiary according to item (2) of this article, and the transfer can be tracked in the beneficiary's country.

5. The concerned person (the transferring institution) in case transfers are local, commits to any of the following;

a. Include payment instructions related to fund transfers or telegraphic transfers, specifying the transferor's account number and, if no account number exists, providing unique transaction reference details. Additionally, include the transferor's address or national identity number, such as ID card, passport number, or date and place of birth.

b. Include payment instructions related to fund transfers or telegraphic transfers, specifying the transferor's account number and, if no account number exists, providing unique transaction reference details. Provided that the details enable to trace the transaction to determine the initiator and the beneficiary and to provide the details to SCA and law enforcement authorities.

6.The person in question (the transferring institution) should retain a record of the transferor and beneficiary.

7. Refrain from executing financial telegraphic transfers if unable to comply with Article 1 of this section.

Article (2) The beneficiary

1. The entity receiving funds must undertake reasonable measures, including monitoring beyond the event or real-time monitoring where possible, to identify cross-border financial transfers lacking necessary information about the transferor or beneficiary.

2. For cross-border fund transfers, the concerned person (the receiving institution) is obligated to identify the beneficiary and verify their identity, ensuring that the identification is not previously established and confirming it as needed.

Article 3: The Intermediary Institution

1. The person in question (the intermediary institution) is committed to retaining all required information about the transferor and the accompanying beneficiary for cross-border fund transfers.

2. If technical constraints prevent the necessary information about the transferor or beneficiary and the accompanying details for cross-border fund transfers from being kept, the concerned person (the intermediary institution) must retain a record for a minimum of ten years, containing all information received from the transferring institution or another intermediary institution.

3. The person in question (the intermediary institution) is obligated to take reasonable measures, in line with direct processing, to identify cross-border financial transfers lacking the required information about the creator or beneficiary.

Article 4: Travel Rule

1. Providers of virtual asset services and relevant individuals involved in the transfer, sending, and receipt of virtual assets must adhere to the provisions of this section and the recommendation (16)

along with its interpretative note from the Financial Action Task Force.

2. The concerned person is committed to providing technological solutions to effectively and efficiently comply with the Travel Rule, incorporating the following key measures:

a. Identify the relevant counterparties concerning virtual assets.

b. Provide accurate information from the transferor and necessary information about the beneficiary, including their respective account numbers and the address of the virtual asset wallet, immediately upon the transfer of virtual assets on a distributed ledger platform.

c. Handle a significant and reasonable number of transactions to various destinations in a stable and efficient manner.

d. Securely transfer data mobility, by ensuring the protection and availability of information to facilitate record-keeping securely.

e. Safeguard the use of recipients from relevant individuals and other obligated entities for such information, and to protect them from any disclosure to non-authorized persons as per the provisions of confidentiality and data law.

f. To support further monitoring with relevant counterparties, the concerned person commits to exercising care towards each of them and requesting information about a specific transaction to determine whether the transaction involves high risks or prohibited activities.

Article 5: Systems and Controls Related to the Transfer of Funds and Virtual Assets

The concerned person is committed to ensuring that the anti-money laundering compliance program includes policies and risk management procedures that outline the steps to be taken if a fund transfer or transfer of virtual assets lacks the required information under this section, or if it is rejected, blocked, modified, and any necessary follow-up actions.

Chapter Six: Internal Auditing

Article 1: Audit Function

The concerned person is committed to ensuring that:

1. The audit function includes conducting regular reviews and assessments of the effectiveness of its anti-money laundering compliance program and evaluating the extent of compliance with this program.

2. The internal audit function is independent and separate from the processes of assessing the “money laundering” risks related to the preparation, implementation, or maintenance of anti-money laundering compliance programs.

3. The internal audit team consists of qualified specialists with experience, possessing the knowledge and skills necessary to assess the effectiveness of the anti-money laundering compliance program.

4. The internal audit function retains the ability to access all records and necessary personnel to conduct its reviews.

5. The internal audit function retains records of its reviews, results, and recommendations for a period of not less than ten years.

Article 2: Internal Audit Policy and Procedures

The concerned individual is committed to having an internal audit policy for the anti-money laundering compliance program that includes:

1. Clear framework for the implementation and management of Auditing including: Governance, risk assessment, planning and methodology, Preparation of reports and defining the responsibilities of the audit team, the Board of Directors, senior management, and the process of developing the audit program in accordance with the obtained results.
2. Audit policy and procedures for annual planning of audits of the anti-money laundering compliance program, including Scheduling and coordinating audits with other internal or external reviews.
3. Procedures for reporting the results of audits to the Board of Directors and senior management, including any recommendations to improve the compliance program to combat money laundering

Article 3: Scope of Audit

1. The internal auditor of the concerned party shall opt for a comprehensive, limited, horizontal, vertical, or change management audit based on the annual risk assessment results.

2. The internal audit function shall serve as a comprehensive and inclusive reference for the anti-money laundering compliance program of the concerned party at least every two years, including, but not limited to:

- Risk assessment.
- Policies, systems, controls, and procedures.
- Enhanced due diligence measures towards clients.
- Continuous due diligence measures and ongoing monitoring.
- Reports on suspicious activities and transactions.
- Relevant information technology systems supporting the anti-money laundering program.
- Reports on administrative information systems.
- Professional training.
- Record retention.
- Adherence to legal and regulatory requirements.

Article 4: Internal Audit Reports

1. The internal audit function must regularly present its findings and recommendations to the senior management and the Board of Directors (or the owner/partners in the absence of a Board of Directors).

2. The internal audit function shall provide recommendations to address any identified deficiencies or opportunities for improvement addressed during its review.

3. The concerned person must take appropriate action to address any identified deficiencies or opportunities for improvement as determined by the internal audit function.

Chapter Seven: Compliance Officer and Responsibilities for Anti-Money Laundering Reporting

Article 1: Compliance Officer and Responsibilities for Anti-Money Laundering

1. The compliance officer is responsible for implementing the anti-money laundering compliance program, in addition to supervising on a daily basis the compliance with relevant laws and regulations and the execution of the provisions of this section.

2. The concerned person must ensure that the role of the compliance officer is not shared with any other operational functions and should be limited to tasks related to compliance with the applicable laws in the country.

3. The concerned person must ensure that the compliance officer is a resident in the country, suitable for the duties, and possesses an appropriate level of experience, competence, and independence for this role.

4. In the event of the absence or vacancy of the compliance officer position, the concerned person must appoint a temporary substitute according to the following:

- a. The substitute must be a full-time employee.
- b. The substitute should not engage in any part-time work or work as an external consultant outside the scope of the concerned person's business.
- c. The substitute must be a resident in the country.
- d. The substitute employee must meet the conditions specified in the Financial Activities Rulebook (Chapter Two/Article 5).

Article 2: Characteristics and Authorities of the Compliance Officer

The concerned person commits to enabling the compliance officer to perform their duties, as outlined below, including but not limited to:

1. Direct access to senior management.

2. Providing adequate resources, including ensuring a suitable number of trained staff to assist in performing duties effectively, objectively, and independently.

3. Granting timely and unrestricted access to sufficient information.

Article 3: Responsibilities of the Compliance Officer

The concerned person commits to ensuring that the compliance officer executes and oversees matters outlined below:

1. Daily operations regarding the person's commitment to the compliance program to combat money laundering.

2. Acting as an internal point of contact to receive reports from employees in case they become aware or suspect, with reasonable grounds, the involvement of an individual in money laundering. Taking appropriate action upon receiving notification from employees under Article 2 of Chapter Ten.

3. Serving as a liaison between the concerned person and the Authority and relevant bodies in the State.

4. Promptly providing reports on suspicious transactions, suspicious activity reports, or other types of reports in accordance with federal legislation to combat money laundering.

5. Responding promptly to requests from the Authority or relevant authorities in the State to obtain information.

6. Receiving any results, recommendations, directives, decisions, penalties, notifications, observations, or other conclusions.

7. Maintaining appropriate training for employees in the field of money laundering and developing sufficient training programs and awareness arrangements.

8. Preparing a semi-annual report on the effectiveness of internal controls according to the approved procedures of the Authority.

Article 4. Collaboration between the Compliance Function and the Internal Audit Function.

To ensure effective oversight and risk management, the concerned person commits to ensuring integration, cooperation, and coordination between the compliance function and the internal audit function.

Chapter Eight: Targeted Financial Sanctions and Other International Measures

Article 1: United Nations Resolutions and Related Sanctions

Every person commits to the following:

1. Developing and updating policies, systems, and controls and retaining them to ensure on an ongoing basis that they are aware of United Nations decisions and sanctions, taking reasonable measures to comply with the decisions or related sanctions.

.2 Notify the Authority, and the executive office of supervision, and prohibition of dissemination, Immediately and in accordance with applicable regulations in case of being aware that a financial transaction is about to be executed or has been executed on or for or on behalf of a person who retains or will retain the funds or assets of someone. This includes any actions that violate the decisions and sanctions of the United Nations Security Council related to the matter.

.3 Ensure that the notification in clause (2) is correct, provided that it includes a description and information about the specific case and the action proposed to be taken or has been taken. .

.4 Take reasonable measures to comply with the decisions or sanctions of the United Nation's Security Council, for example, the commitment of the involved person not to engage in any transaction for or on behalf of a person or to conduct further due diligence in relation to that person who constitutes a violation of the decisions and sanctions of the Security Council.

.5 Exercise due diligence to ensure that the funds are not involved in any financial activity that facilitates the laundering of funds.

.6 Exercise due diligence to ensure that activities related to the collection of funds or the inclusion of persons involved in “money laundering” are not facilitated.

.7 Pre-check decisions or sanctions issued by the United Nations Security Council and taking the necessary legislative actions.

Article (2) Government, regulatory and international outcomes

.1 The concerned person is committed to developing and updating internal policies related to the compliance program for combating money laundering and retaining them. This includes considering all relevant government, regulatory, and international decisions, findings, sanctions, recommendations, guidelines, and warnings issued by:

a. The government of the United Arab Emirates or any governmental bodies within it.

b. The Securities and Commodities Authority.

c. The Central Bank of the United Arab Emirates or the Financial Intelligence Unit.

d. Law enforcement agencies in the United Arab Emirates.

e. The Financial Action Task Force (FATF).

2.The result or results referred to in paragraph 1 of this article include measures that the concerned person must adhere to. This includes, for example, but not limited to:

a. Specifying enhanced due diligence elements.

b. Requesting enhanced or risk-based procedures for financial transactions.

c. Limiting business relationships or financial transactions with specific individuals or entities in a designated country.

d. Prohibiting relevant persons from relying on third-party introducers located in a specific country or regulatory Authority.

e. Banning the execution of specific electronic financial transactions.

f. Increasing the external audit requirements for the financial group concerning branches and subsidiaries located in a specific country or regulatory Authority.

The concerned person is committed to immediately notifying the Authority when aware of the presence of a non-compliant person with government, regulatory, or international results, providing sufficient information about that person, and stating the nature of the non-compliance.

Chapter Nine: Training and Awareness

Article 1: Training Policy

The concerned person must have a comprehensive training policy covering all aspects related to combating “money laundering,” including required types of training, training frequency, and targeted employees.

Article 2: Training Needs Analysis

The concerned person must, before developing the training plan, conduct a training needs analysis for their employees to identify the requirements related to their roles, responsibilities, and the level of exposure to risks within the specified training framework for each employee.

Article 3: Responsibilities of the Person in Charge of Training and Awareness

The person in charge must commit to the following:

1. Providing comprehensive training on the Anti-Money Laundering (AML) program to all relevant employees regularly.

2. Ensuring that training enables employees to:

- Understand relevant legislation related to AML.

- Understand the AML program and any changes to it.

- Identify and handle transactions and activities related to money laundering.

- Understand the types of businesses and services that may constitute suspicious activities and transactions in the course of its business, that require reporting to the Compliance Officer.

-Understand the procedures for reporting to the compliance officer.

- Recognize techniques, methods, and prevalent trends in money laundering.

- Understand the roles and responsibilities of employees in AML and the responsibility of the compliance officer or his substitute.

- Grasp the outcomes, recommendations, guidance, or other conclusions related to the AML program.

3. Ensuring that the training program is designed appropriately for its activities, including products, services, clients, distribution channels, business partners, and assessing the varying levels of risks associated with money laundering and related weaknesses.

4. Providing necessary and appropriate training for the AML compliance program to all newly joined employees within 30 days from their date of joining.

5. Restricting newly joined employees from independently serving any client until they successfully complete their training.

6. Evaluating the effectiveness of the training program, making improvements as necessary, and conducting this evaluation regularly or when there are changes in federal legislation to combat money laundering and in the AML compliance program.

Chapter Ten: Suspicious activities and transactions Reports

Article 1: Reporting Requirements

The person in charge must adhere to developing and maintaining an Anti-Money Laundering (AML) compliance program to achieve the following:

1. Monitoring and detecting activities or transactions related to potential or other financial crimes associated with money laundering.

2. Providing a detailed Statement of the procedures related to notifying the compliance officer in case an employee becomes aware of, suspects, or has reasonable grounds to believe that an involved person is attempting money laundering within the context of their usual business activities.

3. Explicitly outlining roles, responsibilities, and reporting lines, including documenting these roles, responsibilities, and reporting lines, and elevating reports to the Board of Directors and senior management.

4. Establishing a detailed process to identify unusual or potentially suspicious activities, investigating them, reporting and escalating suspicious transactions and activities to the compliance officer for further review, and submitting possible reports on suspicious activities. This

should include procedures documenting the decision-making process regarding closure or immediate escalation of the suspicious transaction.

Article 2: Suspicious activities and transactions Reports

The person in charge commits to the following:

1. Upon receiving a notification under section 2/1 of this chapter, the compliance officer must take the specified actions as outlined below:

a. Inquire into and document the circumstances related to the submitted notification.

b. Determine whether it is necessary to report the details of the activity and suspicious transactions to the Financial Intelligence Unit, documenting this decision.

2. Document the reasons if the compliance officer decides not to report suspicious activities.

3. Ensure that if the compliance officer decides to report a suspicious transaction, the decision made is independent and subject to approval or endorsement by any relevant person

4. The person in question should not submit defense reports about suspicious activities when there are doubts or reasonable grounds for suspicion, noting that the submission of such reports indicates the inefficiency of the transaction monitoring system and the weakness of the anti-money laundering compliance program in place.

5. Submit the report of suspicious activities to the Financial Intelligence Unit through the approved channels, following the federal laws for combating money laundering.

Article 3: Confidentiality in Dealing with Reports

1. The concerned person must commit to maintaining the confidentiality of all information reported and the reporting process itself, ensuring the protection of reported information and data from unauthorized access.

2. The person in question should ensure the confidentiality of all relevant information concerning suspicious transactions reports, suspicious activity reports, and other types of reports. This should be done considering the conditions and exceptions specified in federal laws for combating money laundering. Guidelines for this should be incorporated into the person's anti-money laundering compliance program.

3. The confidentiality requirement does not apply to the exchange of information within the person in question or its affiliated entities (such as foreign branches or subsidiaries) related to transactions and suspicious crimes in the field of money laundering.

4. If the person in question suspects the commission of a crime, they may choose not to apply due diligence measures towards their client or potential client if they have reasonable grounds to believe that applying such measures could alert the client or potential client. They are allowed to opt-out of pursuing this transaction, and

they must report suspicious activity to the Financial Intelligence Unit. The person should ensure that their employees are aware of these matters and their sensitivity when performing due diligence.

Article 4: Customer Relationship Termination Policy in Suspicious Cases

The concerned person must have a policy for terminating the business relationship with clients. This policy should outline the review process of such relationships, specify the necessary steps to terminate these relationships, and report them to the relevant authorities if required.

Chapter Eleven: Compliance Commitments

Article 1: General Compliance Commitments

1. The responsibility for compliance is with every member of the board of directors and every member of the senior management, as well as the compliance officer.

2. The senior management is committed to exercising due care in fulfilling its duties under this chapter.

3. The person in question, along with members of the board and senior management, and employees, must be aware of their obligations regarding federal anti-money laundering legislation and criminal law in the country.

4. The person in question, members of the board, senior management, and employees bear criminal responsibility for specific behaviors, including but not limited to:

a. Money laundering.

b. Financing terrorism.

c. Financing illegal organizations.

d. Reporting a suspicious transaction or activity.

e. Evading targeted financial sanctions.

5.The person in question commits to freezing assets or funds in accordance with the federal legislation to combat money laundering.

Article 2: Financial Group

The concerned person must commit to :

1. Ensure that the anti-money laundering compliance program applies to subsidiaries and affiliated companies, and to disseminate and maintain the compliance program throughout the financial group.

2. When anti-money laundering requirements differ in another country or regulatory Authority from the legislation of the Authority or the State, the branch or subsidiary in that country or under that regulatory Authority is required to apply the higher of the two standards, to the extent permitted by the laws of that country or regulatory Authority, documenting the basis upon which this determination is made.

3.In the event that the laws of another country or regulatory Authority do not permit the enforcement of federal legislation combating money laundering on the branch of the concerned person or its subsidiary in that country or under that regulatory Authority, they must take the following actions:

A. Notify the Authority in writing.

B. Implement additional measures suitable for managing the money laundering risks related to the relevant branch or subsidiary.

Article 3: Financial Group Policies

1. **The concerned person, when part of the financial group, commits to ensuring that:**

    A. Develops and implements policies and procedures for sharing information among entities within the financial group, including sharing information related to due diligence on customers and risks of money laundering.

    B. Has sufficient assurances regarding the confidentiality and use of information exchanged between entities within the financial group, including considering relevant data protection laws.

    C. Maintains continuous awareness of the risks of money laundering that the financial group is exposed to and has effective controls to mitigate these risks.

    D. Contributes to assessing risks at the level of the financial group to identify and evaluate the risks of money laundering for the group.

    E. Provides, at the level of the financial group, compliance functions and auditing to combat money laundering and provides information on customer accounts and transactions

at branches and subsidiaries when necessary and for anti-money laundering purposes.

2.The concerned person commits to notifying the Authority as soon as possible when engaging in activities or concerning its branches or subsidiaries in the event of:

A. Receiving a request for information from a regulatory Authority or an agency responsible for combating money laundering, related to investigations into potential money laundering operations, financing terrorism, or violations of sanctions.

B. Being aware of any matter related to money laundering associated with the person concerned or any members of their group, knowing about non-compliance with the provisions of this section or federal laws for combating money laundering by the person concerned or any members of their board, senior management, or any of their employees.

Chapter Twelve: Final Provisions

Article 1: Record Retention

1. The concerned person is committed to retaining records for ten years from their date in an organized manner allowing data analysis and tracking financial transactions. These records should

be made available to the Authority and other competent authorities upon request promptly.

The concerned person, at a minimum, commits to retaining:

a- Copies of all documents and information obtained during the due diligence measures towards clients, including the results of the inquiry and verification before initiating any business relationship with the client.

b- Records consisting of original documents or certified copies regarding the business relationship with the client, including:

1) commercial correspondences and other information related to the client's account.

2) Adequate records for individual transactions to enable the reconstruction of specific transactions.

3) Internal results and analyses related to a transaction or any business activity, especially if it is unusual or suspicious, leading to the reporting of suspicious activity or money laundering or not.

c - All internal notifications sent to the compliance officer.

d- Reports of suspicious activities and any related supporting documents, including internal results and analyses.

e- Any communications with the financial information unit.

f- Business risk assessment reports and the methodology followed for risk assessment.

g- Evaluation of the client's money laundering risks, the decision made regarding its classification, and the methodology followed for risk assessment.

h - Training and awareness records for its employees.

i - Any other reports required or requested by the concerned person under this section.

2. The concerned person must verify whether there is any legislation related to confidentiality or data protection that restricts access to the mentioned records.

Article 2: Annual Anti-Money Laundering Risk Assessment Acknowledgment

1. The concerned person commits to completing the acknowledgment of the annual "Anti-Money Laundering" risk assessment according to the prepared forms or the dedicated electronic system for this purpose by the Authority and within the specified deadlines.

2. The concerned person is committed to ensuring that the data and information in the acknowledgment are accurate and precise.

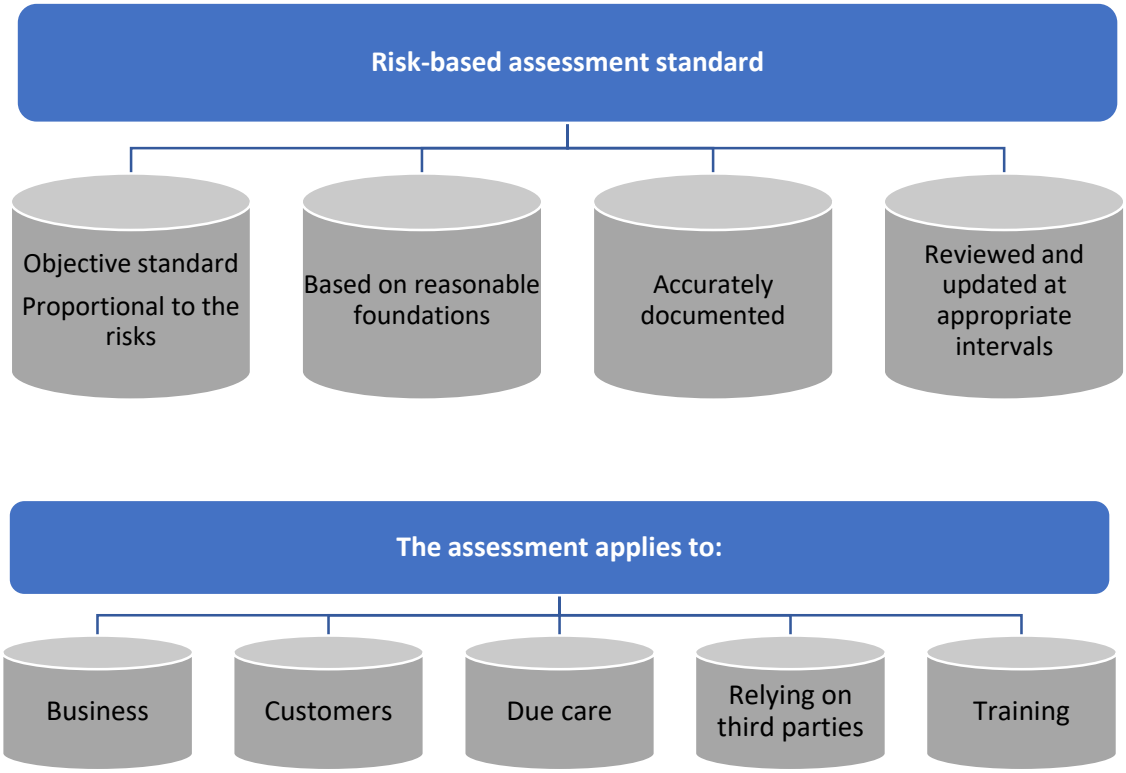
Article 3: Employee Disclosures

The concerned person is committed to ensuring the protection and confidentiality of the employee's data when the employee discloses any information related to "Anti-Money Laundering" to the Authority or any other relevant official entity involved in combating "Money Laundering."

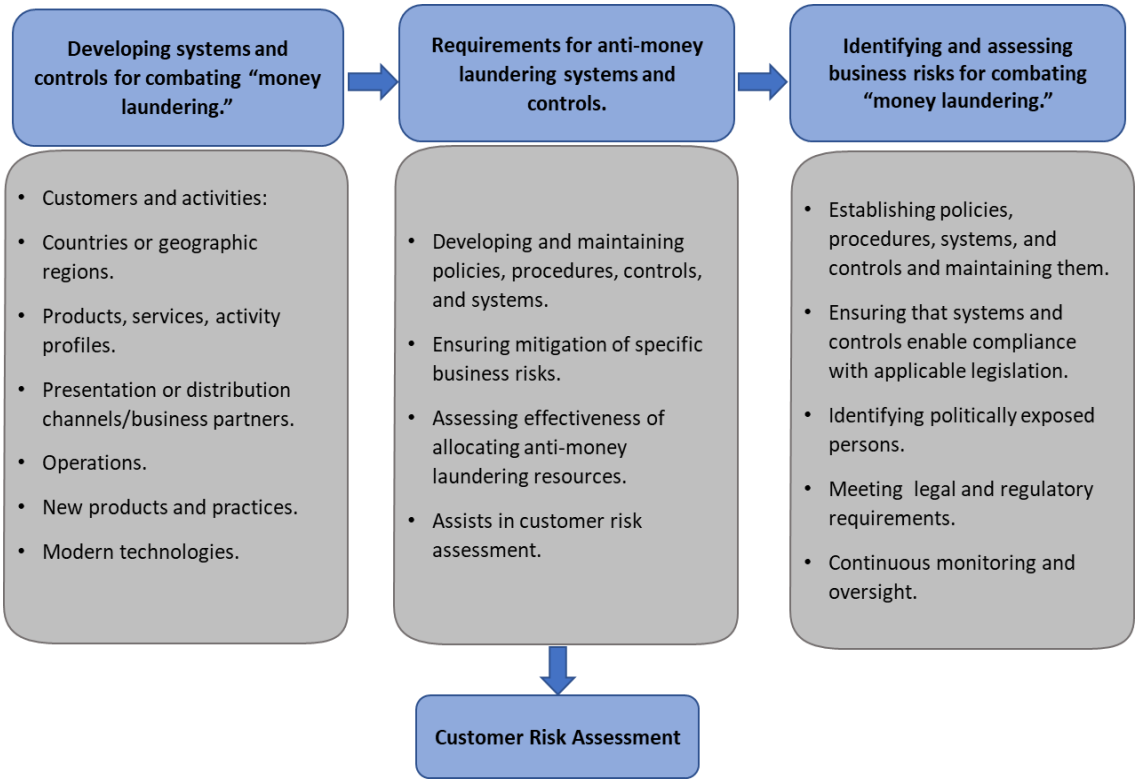
Article 4: Penalties

The administrative and financial penalties stipulated in Federal Law Decree No. 20 of 2018 apply in the event of violations by the concerned person, its board members, senior management, any of its employees, or any individual proven responsible for violating the provisions of this chapter and federal laws combating money laundering.

The attachment number (1) – Illustration of The Risk-based Approach

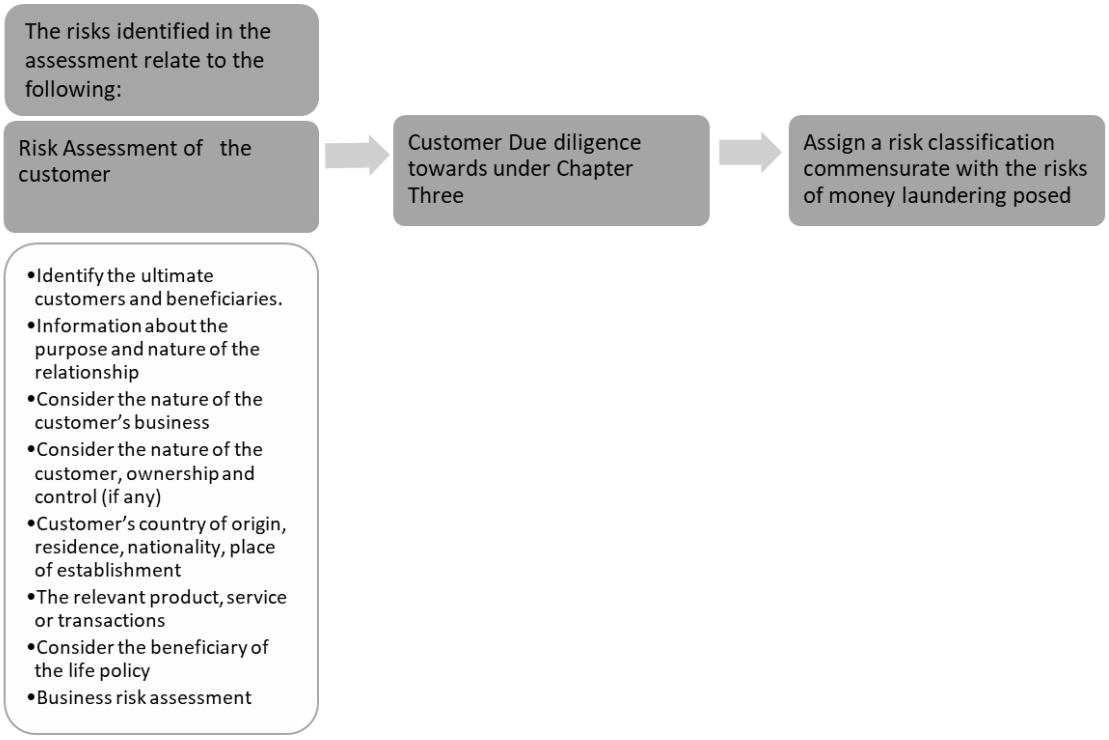


Attachment number (2) – Illustrative diagram for business risk assessment

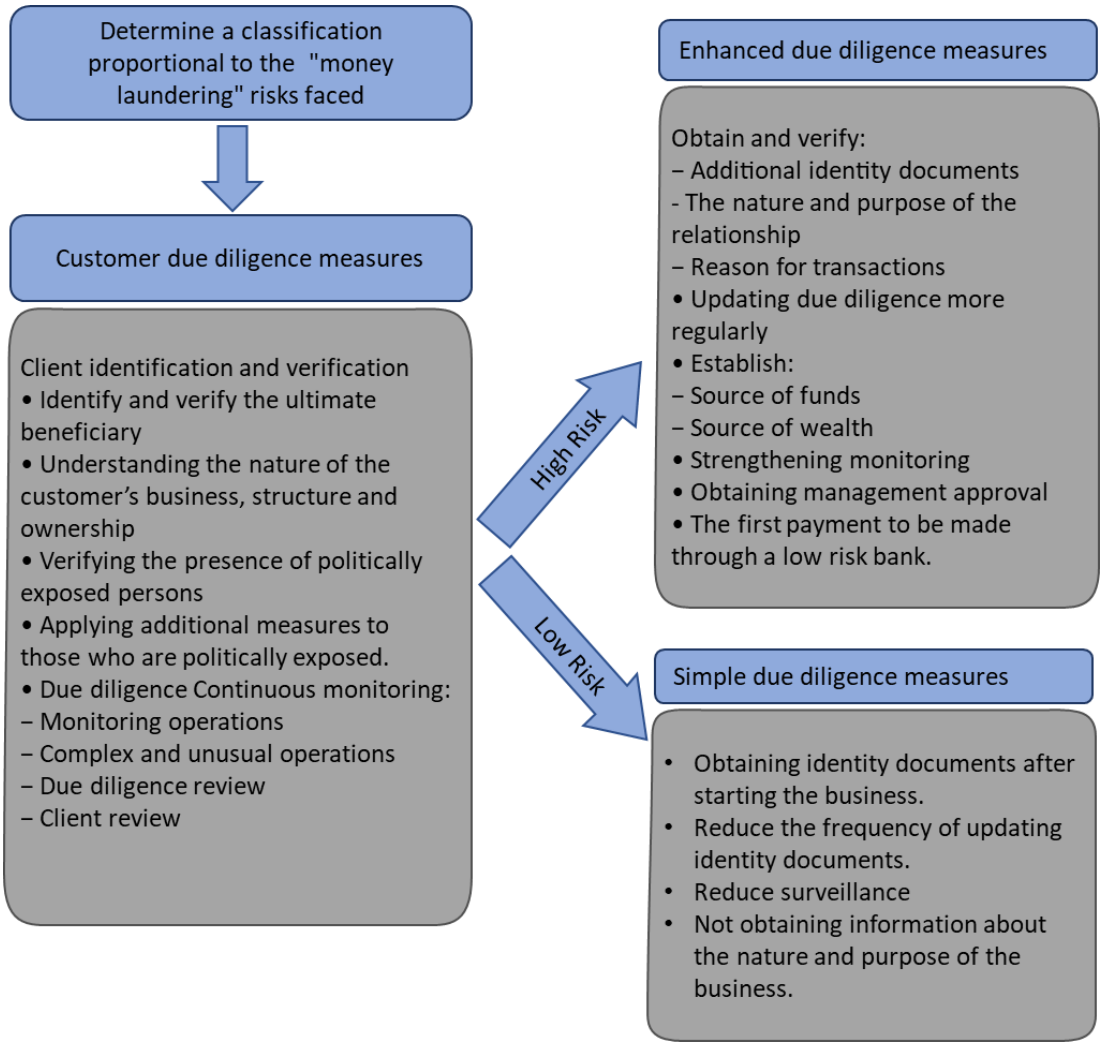


Attachment 3

Illustrative diagram for customer risk assessment



Attachment 4: Illustration of customer due diligence measures



Attachment 5 Illustration of dependence on third part