Financial Market Council Regulation on practical measures for combating money laundering , combating the financing of terrorism and the proliferation of weapons[1]

The Financial Market Council,

Having regard to Organic Law No. 2015-26 of August 7, 2015 on combating terrorism and suppressing money laundering, and in particular Articles 107 and 115 thereof,

Having regard to Law No. 94-117 of November 14, 1994, on the reorganization of the financial market, as amended and supplemented by subsequent texts, and in particular by Law No. 2009-64 of August 12, 2009, promulgating the code for the provision of financial services to non-residents, and in particular Articles 28, 29, 31, 40, and 48,

Having regard to Decree No. 99-2478 of November[1,] 1999, on the status of stockbrokers, as amended and supplemented by Decree No. 2007-1678 of July 5, 2007, and in particular Articles 50 bis, 65 bis, 86 new, and 86 bis,

Having regard to Decree No. 2006-1294 of May 8, 2006, implementing the provisions of Article 23 of Law No. 2005-96 of October 18, 2005, on strengthening the security of financial relations, as amended and supplemented by Decree No. 2009-1502 of May 18, 2009, and in particular Articles 6 and 6 ter thereof,

Having regard to the Financial Market Council's regulations on undertakings for collective investment in transferable securities and the management of securities portfolios on behalf of third parties, referred to in the order of the Minister of Finance of April 29, 2010, as amended and supplemented by the order of the Minister of Finance of February 15, 2013, and in particular Articles 82, 84, and 152.

Decides:

[1]As referred to in the order of the Minister of Finance dated January 19, 2017, and amended by the order of the Minister of Finance dated March 6, 2018.

Article 1:

This regulation sets out the practical measures to be applied, for the suppression of money laundering and the fight against terrorist financing, by:

- stockbrokers,

- securities portfolio management companies acting on behalf of third parties.

Hereinafter referred to as "institutions."

Article 2:

For the purposes of this regulation, the following definitions apply:

- **Customer:** a customer of the institutions, whether regular or occasional, a natural person or a legal entity. An occasional customer is any person who contacts the institutions for the purpose of preparing or carrying out a one-off transaction or operation. A one-off transaction or operation is one that does not give rise to the establishment of an account opening or management agreement.

- **Legal entity:** any entity with its own resources and assets that are separate from those of its members or partners, even if it has not been granted legal personality under a specific law.

- **The beneficial owner:** the natural person who ultimately owns or controls the customer or on whose behalf a transaction or operation is carried out, even in the absence of a written mandate between the customer and the beneficial owner.

- **Reliable and independent sources:** central or local official authorities or financial institutions established in a country that sufficiently applies international standards for the prevention of money laundering and the fight against terrorist financing.

- **Electronic transfer:** any electronic funds transfer operation within the meaning of Law No. 2005-51 of June 27, 2005, on electronic funds transfers.

- **Persons exposed to risks due to their functions:** persons who hold or have held, in Tunisia or in a foreign country, up to the year preceding the establishment of the business relationship, high public office or representative or political positions, in particular:

1. Head of State, head of government or member of a government,
2. Member of parliament,
3. Member of a constitutional court or high court whose decisions are not subject to appeal,
4. Member of a constitutional body,
5. Senior military officer,
6. Ambassador, chargé d'affaires, or consul,
7. Member of the governing bodies of supervisory and regulatory authorities,
8. Member of an administrative, management, or supervisory body of a public enterprise,
9. Member of the governing bodies of an international institution established by treaty or the head of its representation,
10. Senior official of a political party,
11. Member of the governing bodies of a trade union or employers' organization.

- **The Financial Action Task Force:** an intergovernmental body whose objectives include developing standards and promoting policies for combating money laundering and terrorist financing.

- **Suspicious transactions and operations:** transactions and operations that raise suspicion of being directly or indirectly linked to funds derived from illegal acts classified by law as misdemeanors or crimes, or to the financing of persons, organizations, or activities related to terrorist offenses as defined by Organic Law No. 2015-26 of August 7, 2015, on combating terrorism and money laundering, as well as any attempt to carry out such transactions or operations.

- **The commission:** the Tunisian Financial Analysis Commission provided for in Article 118 of Organic Law No. 2015-26 of August 7, 2015, on combating terrorism and money laundering.

- **Fictitious foreign correspondent**: a foreign bank or financial institution that does not have a fixed head office from which to conduct its business and is not subject to the supervision of a regulatory authority. This definition does not apply to institutions affiliated with a bank or financial institution that is authorized and subject to supervision by a regulatory authority established in a country that adequately applies international standards for the suppression of money laundering and the fight against terrorist financing.

- **Organization**: a structured group of three or more persons, formed for any period of time and acting in concert with the aim of committing one of the offenses provided for by Organic Law No. 2015-26 of August 7, 2015, on combating terrorism and suppressing money laundering within the national territory or abroad.

- **Designated person or entity:** Any natural or legal person or entity designated for the application of targeted financial sanctions related to the financing of the proliferation of weapons of mass destruction pursuant to United Nations Security Council resolutions and whose names appear on the list drawn up by the competent national authority having legal authority. (*Decree of the Minister of Finance of March 6, 2018)*

- **Targeted financial sanctions:** include both the freezing of funds and other assets of a designated person or entity and prohibitions aimed at preventing funds and other assets from being made available, directly or indirectly, to or for the benefit of that person or entity. *(Decree of the Minister of Finance of March 6, 2018)*

- **Competent national authority with legal authority:** the national authority or authorities designated by law and responsible for implementing and enforcing targeted financial sanctions. *(Decree of the Minister of Finance of March 6, 2018)*

Chapter I

Customer due diligence measures

Article 3:

Institutions must refrain from opening anonymous accounts or accounts under fictitious names.

When establishing a business relationship, they must verify, using official documents and other documents from reliable and independent sources, the customer's full identity, activity, address, and the purpose and nature of the business relationship, and record all necessary data that could identify the customer. When the customer appoints a person to represent them, institutions must verify that person's full identity and obtain data proving their relationship with the customer, even if the appointment took place after the business relationship was established.

In the case of an occasional customer, the obligation to verify identity applies when they carry out occasional financial transactions or operations whose value is equal to or greater than the amount set by the regulations in force, or in the form of electronic transfers, whether these are carried out in a single operation or in several related operations.

Institutions must also comply with the obligation to verify identity when:

- there is suspicion of money laundering or terrorist financing,
- there are doubts as to the accuracy or relevance of the customer identification data previously obtained.

The obligation to verify the customer's identity does not apply to companies listed on the Tunis Stock Exchange and public companies.

Article 4:

If circumstances surrounding the transaction or operation indicate that it is being carried out or could be carried out for the benefit of a third party, the obligation on institutions to verify identity also extends to the beneficial owner of the transaction or operation.

third party, the obligation to verify identity incumbent upon institutions shall also extend to the beneficial owner of the transaction or operation.

Article 5:

Without prejudice to the procedures for opening accounts for clients provided for in the regulations governing the financial market, institutions must, at a minimum, collect the following data when identifying the client, their representative, and the beneficial owner:

In the case of a natural person:

- Full name, date and place of birth, and nationality,
- The identity card or passport number, date of issue and expiry date,
- The address of the actual place of residence, including the postal code, telephone number, and, where applicable, email address,
- Occupation and address,
- The purpose and nature of the business relationship,
- A specimen signature.

The above data is verified on the basis of the national identity card for Tunisians and an official identity document recognized by the Tunisian authorities, including the photo, address, and occupation of the holder for foreigners.

In the case of a legal entity:

- The date of its incorporation, its business name or company name, its legal form, and its corporate purpose,
- The registration number in the commercial register and the tax identification number,
- Address of the registered office, including the postal code, telephone and fax numbers, and email address. When the main activities are not carried out at the registered office, the actual address where the activity is carried out must be indicated.
- Breakdown of capital,
- Identity of its directors and persons authorized to act on its behalf, as well as documents proving their capacity to do so, with the obligation to

collecting, in relation to them, the data relating to natural persons provided for in this article,

- Identities and addresses of the main shareholders whose shareholding in the company amounts to at least 40% and of the persons who control it in the case of a company or, if it is an entity other than a company, the identity of the constituents and persons who exercise effective control or who are the beneficial owners, with the obligation to collect, in their regard, the data relating to natural persons provided for in this article,
- The purpose of the business relationship and its nature.

The above data shall be verified on the basis of the articles of association, an extract from the commercial register, a deed of incorporation, and any equivalent official document or any other document from reliable and independent sources, where the legal entity is registered abroad.

Institutions must consult the original documents on the basis of which the data referred to in this article have been verified and obtain copies of them, which must be kept in a file specific to each customer.

Article 6:

Institutions must take the necessary measures to verify, at the time of establishing the business relationship or carrying out a transaction or occasional operation, and periodically thereafter, that the customer or beneficial owner is not on the list of persons or organizations whose connection with terrorist crimes has been established by the competent international bodies or by the national counterterrorism commission provided for in Article 66 of Organic Law No. 2015-26 of August 7, 2015, on combating terrorism and money laundering.

They must also freeze the assets belonging to the persons or organizations referred to in the first paragraph of this article and make the relevant declaration, in accordance with the provisions of Article 103 of Law No. 2015-26 of August 7, 2015, on combating terrorism and money laundering.

Article 6 (bis): *(Decree of the Minister of Finance of March 6, 2018)*

Institutions must take the necessary measures to verify, at the time of establishing the business relationship or carrying out a transaction or occasional operation and periodically thereafter, that the customer or beneficial owner is not listed on the list of persons or entities subject to targeted financial sanctions relating to the prevention, suppressing and interrupting the proliferation of weapons of mass destruction and its financing, as determined by the competent national authority with legal authority.

Institutions must also:

- freeze, without delay and without prior notification, the funds and other assets of designated persons and entities. The freezing obligation shall extend to:

• all funds or other assets owned or controlled by the designated person or entity, and not only those that may be specifically related to an act, plot, or threat of weapons proliferation,

• funds or other property owned or controlled, wholly or jointly, directly or indirectly, by the designated person or entity,

• funds or other property derived from or generated by funds or other property owned or controlled, directly or indirectly, by the designated person or entity,

• funds or other property of natural or legal persons acting on behalf of, or at the direction of, the designated person or entity.

- refrain from making funds and other assets available to the designated person or entity, unless authorized by the competent national authority having legal authority,

- report to the competent national authority with legal authority all frozen funds or other assets and all measures taken in accordance with the prohibitions imposed by it, including attempted transactions.

Article 7:

Institutions must regularly update data and documents relating to the identity of their customers and exercise ongoing vigilance with regard to them throughout the duration of the business relationship. The

frequency of updates shall be determined on the basis of the volume of transactions and operations carried out by the institutions and the degree of risk to which they are exposed.

Article 8:

Upon publication of this regulation, institutions must take the necessary measures to comply with the provisions relating to customer identity verification with respect to customers with whom they have established a prior business relationship, taking into account the degree of risk posed by these customers with regard to their identity and the nature of the transactions they carry out, as well as the relevance of the data previously collected about them.

Article 9:

Institutions that use a third party to establish business relationships or carry out occasional transactions or operations must:

- Ensure that the third party is subject to legislation and supervision relating to the prevention of money laundering and the fight against terrorist financing,
- Specify in writing the procedures to be put in place to verify the identity of customers in accordance with the provisions of this regulation and ensure compliance with them,
- Obtain customer identification data without delay,
- Ensure that it is able to provide, upon request and as soon as possible, copies of the documents used to verify the identity of customers and other related documents.

Where institutions use a third party belonging to the same group, they must ensure that the entities within the group apply due diligence measures and procedures for the prevention of money laundering and terrorist financing that cover the use of a third party to establish business relationships or carry out occasional transactions or operations.

Where recourse to a third party gives rise to the establishment of an agreement, the latter must mention the obligations incumbent on the third party as provided for in indents 2 to 4 of the first paragraph of this article.

Where institutions have been unable to take the due diligence measures provided for in the first and second paragraphs of this article, they must refrain from using the third party.

In any event, the use of a third party does not exempt institutions from their responsibility to comply with the provisions in force relating to the prevention of money laundering and the fight against terrorist financing, and more specifically their responsibility to verify the identity of customers.

Article 10:

Institutions must exercise particular vigilance with regard to business relationships that do not involve the physical presence of the parties.

As such, they must:

- Compare the data collected from the customer with other data from reliable and independent sources,
- Arrange a face-to-face meeting with the customer as soon as possible,
- Require the customer to carry out their first financial transactions through a bank established in a country that adequately applies international standards for the prevention of money laundering and the fight against terrorist financing in accordance with the decisions of the Financial Action Task Force.

Article 11:

Institutions must exercise particular vigilance with regard to business relationships with persons exposed to risks due to their positions and with their spouses, ascendants, and descendants up to the first degree, as well as with persons closely associated with them, in particular those who have close business ties with them.

In this regard, institutions must:

- Establish procedures to verify whether the customer, their representative, or the beneficial owner belongs to the category of persons referred to in the first paragraph of this article.
- Obtain authorization from the administrative or management bodies or persons authorized for this purpose to establish or continue a business relationship with the persons referred to in the first paragraph of this article.
- Establish procedures to determine the origin of funds of the persons referred to in the first paragraph of this article,
- Subject transactions and operations carried out by the persons referred to in the first paragraph of this article to enhanced and ongoing monitoring.

Article 12:

Where institutions are unable to verify the information referred to in Article 5 of this Regulation, or where such information is insufficient or clearly fictitious, they shall refrain from opening the account, establishing or continuing the business relationship, or carrying out the transaction or operation, and shall consider making the report referred to in Article 18 of this Regulation.

Article 13:

Institutions must refrain from accepting cash deposits whose value is equal to or greater than the amount specified in the regulations in force, even if made in several payments that may be linked. They must also refrain from accepting checks or bank transfers that are not issued by the customer or their representative.

Chapter Two

Vigilance measures with regard to transactions and operations

Article 14:

Institutions must carefully examine the transactions and operations carried out by their customers to ensure that they are consistent with the data they have on them, taking into account

the nature of their activities, the risks they incur, and, where applicable, the origin of their funds.

Article 15:

Institutions must exercise particular vigilance with regard to unusual transactions and operations, in particular those that are:

- Complex in nature,
- involving an abnormally high amount,
- Whose economic purpose or legality is not immediately apparent,
- Not appearing consistent with the customer identification data,
- Carried out by persons established in countries that do not apply or insufficiently apply international standards for the prevention of money laundering and the fight against terrorist financing and that are reported in the communiqués of the Financial Action Task Force.

Institutions must carefully examine the context in which unusual transactions or operations are carried out, as well as their nature, and, where appropriate, request additional information concerning the reason for the transaction or operation and the origin of the clients' funds, in order to determine that they are not suspicious transactions or operations. The results of the examination must be recorded in writing in a register kept for this purpose.

Article 16:

Institutions must take the necessary measures to identify and assess the risks of money laundering and terrorist financing associated with the development of new products and services or the use of new technologies. Where necessary, they must update the rules and procedures relating to the prevention of money laundering and terrorist financing.

Article 17:

Institutions must exercise particular vigilance with regard to transactions and operations carried out via electronic transfers, particularly when:

- The electronic transfer order is given by an occasional customer,
- or electronic transfers are carried out in bulk as part of transactions or operations provided for in Article 15 of this Regulation.

Institutions must include in all electronic transfers and related documents relevant information about the transaction or operation concerned, as well as about the customer who gave the transfer order and the customer who is the beneficiary, in particular their full identity in accordance with the provisions of Article 5 of this Regulation and their account numbers.

Where sufficient information concerning an electronic transfer is not available, institutions must decide, based on the degree of risk, whether to refrain from executing or receiving the transfer.

Article 18:

Institutions must immediately submit a written report to the commission, in accordance with the template provided by the commission, on any suspicious transaction or operation. The reporting obligation also applies, even after the transaction or operation has been completed, when new information shows that it falls within the category of suspicious transactions or operations.

Institutions must refrain from disclosing any information concerning the report made and the measures that resulted from it.

Where there is suspicion of money laundering or terrorist financing, and where the implementation of due diligence measures would risk alerting the customer concerned, institutions may immediately make the report provided for in the first paragraph of this article without applying due diligence measures.

Article 19:

Institutions must appoint a commission correspondent and his or her deputy from among their managers or employees. They must notify the commission secretariat of the decision to appoint the correspondent

and his or her alternate, indicating their status, position, telephone and fax numbers, and email address.

The designated persons must have the appropriate hierarchical level, competence, and experience to perform their duties independently and effectively.

The commission correspondent is responsible for reviewing transactions and operations and reporting any that are suspicious. The results of the review are recorded in writing in a register kept for this purpose. Institutions must make available to the commission correspondent all data, documents, and registers necessary for the performance of their duties.

Chapter Three

Required measures in terms of organization, internal control, and continuing education

Section One

Required measures relating to organization

Article 20:

Institutions must have sufficient organizational, technical, and human resources to enable them to comply with the legal and regulatory provisions in force relating to the prevention of money laundering and the fight against terrorist financing. They must establish written rules setting out the procedures to be followed with regard to:

- Verifying the identity of customers and creating and updating their files,
- Reviewing transactions and operations as provided for in Article 15 of this regulation,
- The reporting of suspicious transactions and operations and the non-disclosure of related information,
- The retention of documents.

The written rules must be submitted to the compliance and internal control officer and approved by the management bodies. They must be communicated to the institution's employees, particularly those who are in direct contact with customers.

Article 21:

Institutions must map the risks associated with money laundering and terrorist financing, particularly with regard to the nature of the transactions and operations they carry out and the category of customers with whom they deal. This mapping must be updated regularly.

Article 22:

Institutions must ensure that their branches and subsidiaries established abroad apply the necessary vigilance measures to combat money laundering and terrorist financing. They must immediately inform the Financial Market Council if the legislation of the countries where their branches and subsidiaries are established does not allow for the application of vigilance measures.

Where there is a difference between the due diligence measures provided for in the laws and regulations in force and those applied in the host country, institutions must ensure that their branches and subsidiaries apply the most stringent due diligence measures within the limits permitted by the laws and regulations of the host country.

Article 23:

When institutions establish relationships with foreign correspondents to carry out transactions and operations either on their own behalf or on behalf of their customers, they must implement the necessary procedures to comply with the due diligence measures set out in Article 111 of Organic Law No. 2015-26 of August 7, 2015, on combating terrorism and money laundering.

Institutions must refrain from establishing or continuing a relationship with a fictitious foreign correspondent or with institutions that allow fictitious foreign correspondents to use their accounts.

Article 24:

Without prejudice to the document retention periods provided for in the regulations governing the financial market, institutions must retain customer files and related documents, as well as all documents and information relating to transactions and operations carried out in electronic or paper form, in accordance with the provisions of Article 113 of Organic Law No. 2015-26 of August 7, 2015, on combating terrorism and money laundering.

When institutions use a third party to establish business relationships with customers or to carry out occasional transactions and operations on their behalf, they must ensure that the third party complies with the legal retention periods.

Section Two

Required internal control and continuing education measures

Article 25:

Institutions must establish internal control procedures to verify the effectiveness of measures to combat money laundering and terrorist financing. Control operations must be carried out at a frequency that takes into account the nature, scope, and complexity of the transactions and operations carried out by the institutions.

The rationale for the frequency chosen for conducting control operations and the results of these operations must be recorded in the compliance and internal control officer's report and communicated to senior management.

Article 26:

Institutions must prepare and implement continuing education programs for their employees. These programs must explain the following aspects in particular:

- The laws and regulations in force concerning the prevention of money laundering and the fight against terrorist financing,
- Methods and techniques used in money laundering and terrorist financing and how to detect them,
- The procedures for reporting suspicious transactions and operations and complying with confidentiality obligations,
- The procedures to be followed when dealing with suspicious customers.

Chapter Four

Information obligations towards the Financial Market Council

Article 27:

Institutions must inform the Financial Market Council within one month of the end of each half-year of the number of reports of suspicious transactions and operations made to the commission and their content. This information must be recorded in the compliance and internal control officer's report.

Article 28:

Institutions must submit to the Financial Market Council, within six months of the publication of this regulation, written rules setting out the measures to be taken to combat money laundering and terrorist financing.

They must also submit, within one year of the publication of this regulation, a map of the risks relating to money laundering and terrorist financing. Any updates to this map must be communicated to the Financial Market Council without delay.

Article 29:

Institutions must, without delay, make available to the Financial Market Council, upon request:

- Records containing the results of the analysis of transactions and operations provided for in Article 15 of this Regulation and of suspicious transactions and operations,
- Training programs for their agents in the areas of money laundering and terrorist financing, including details of the content of the training, the date on which it was implemented, and the identity and positions of the agents who participated.

Chapter Five

Sanctions

Article 30:

Without prejudice to other legal and regulatory provisions, any person who violates this regulation is liable to the penalties provided for in Article 40 of Law No. 94-117 of November 14, 1994, on the reorganization of the financial market, as amended and supplemented by subsequent texts.