Council of Ministers' Decision No. [41] of 2019

Promulgating the Implementing Regulations of Law No. (20) of 2019 on Combatting Money Laundering and Terrorism Financing

---

The Council of Ministers,

Having perused the Constitution; and

The Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing; and

The Emiri Resolution No. (29) of 1996 on the Council of Ministers' Decisions submitted to the Emir for Ratification and Issuance; and

The proposal of the Chairman of the National Anti-Money Laundering and Terrorism Financing Committee,

Hereby resolves as follows:

Article (1)

The provisions of the Implementing Regulations of the AML/CFT Law, attached hereto, shall come into force and effect.

Article (2)

All Competent Authorities, each within its own competence, shall implement this Decision, which shall come into force on the day following its publication in the Official Gazette.

Abdulla bin Nasser bin Khalifa Al Thani

Prime Minister

We, Tamim Bin Hamad Al Thani , Emir of the State of Qatar endorse this Decision to be issued.

Emiri Diwan on 29/4/ 1441 corresponding to 26/12/2019

The Implementing Regulations of Law No.(20) of 2019 on Combatting Money Laundering and Terrorism Financing

Chapter 1

Definitions

Article (1)

In the application of this Implementing Regulations, the following words and phrases shall have the meaning assigned thereto, except where the context requires otherwise:

The Law: The Anti-Money Laundering and Terrorism Financing Law, promulgated by Law No. (20) of 2019.

Politically Exposed Persons (PEPs): Individuals who are or have been entrusted by the State or by a foreign State with prominent public functions, such as Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned companies, members of Parliaments, and important political party officials, and members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions in international organizations.

Beneficial owner: the natural person who ultimately owns or controls a customer, through ownership interest or voting rights, or the natural person on whose behalf a transaction is being conducted, whether by proxy, trusteeship or mandate, or by any other form of representation. It also includes any person who exercises ultimate effective control over a legal person or arrangement, including any person excercising ultimate effective control by any means.

Payable-through accounts: correspondent accounts that are used directly by third parties to transact business on their own behalf.

Ordering Financial Institution: the financial institution which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.

Beneficiary Financial Institution: the financial institution which receives the wire transfer from the ordering financial institution directly or through an intermediary financial institution and makes the funds available to the beneficiary.

Intermediary Financial Institution: a financial institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary institution, or another intermediary financial institution.

False declaration: a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is required for submission in the declaration or otherwise requested by customs authorities. This includes failing to make a declaration as required.

Agent for Money or Value Transfer Service (MVTS) Provider: any person providing MVTS on behalf of an MVTS provider, whether by contract with or under the direction of the MVTS provider.

Chapter 2

Activities, Operations and Preventive Measures

Section One

Activities and Operations of Financial Institutions

Article (2)

The Financial Institution conducts, as a business, one or more of the following activities or operations:

1) Accepting deposits and other repayable funds from the public.
2) Lending, including consumer credit and mortgage credit; with or without the right to recourse, financing of commercial transactions, including forfeiting and factoring whether with or without the right to recourse.
3) Financial leasing, except for leasing arrangements related to consumer products.
4) Money or Value Transfer Services, except for providing the financial institutions with support or messaging systems for funds transfer.
5) Issuing or managing means of payment, such as credit and debit cards, cheques, traveller's cheques, transfers, bank cheques, electronic money, money orders, bankers' drafts.
6) Financial guarantees and commitments.
7) Activities related to securities.
8) Trading in :

- Money market instruments, such as cheques, bills, certificates of deposit, and financial derivatives.
- Foreign exchange.
- Currency exchange instruments.
- Interest rate and index instruments.
- Transferable securities.
- Commodity futures trading.

9) Participating in securities issues and providing financial services related to such issues.
10) Management of individual or collective portfolio.
11) Safekeeping and administering cash or liquid securities on behalf of, or for the benefit of, other persons.
12) Investing, administering or managing funds or money on behalf of, or for the benefit of, other persons.

13) Underwriting or placement of life insurance and other investment related insurance; this shall apply to insurance intermediaries (agents and brokers).
14) Money or currency changing.
15) Any other activity or transaction defined by a Decision of the Council of Ministers, upon the proposal of the National Anti-Money Laundering and Terrorism Financing Committee.

Section Two

Preventive Measures

Article (3)

Financial Institutions and Designated Non-Financial Businesses and Professions (DNFBPs) shall identify, assess and understand their ML/TF risks, in accordance with the nature and size of their business, as follows:

1. Document, monitor and regularly update their risk assessments and any key information, in order to be able to provide the basis thereof.
2. Provide the risk assessment report to the competent supervisory authority, on a regular basis and within the time limit set by the supervisory authority, and upon its request.
3. Consider all the relevant risk factors before determining the level and type of mitigation measures to be applied.

Article (4)

Financial Institutions and DNFBPs shall, when identifying risks pursuant to the above Article, consider the risks identified in the National Risk Assessment, in addition to the following factors:

1. risk factors related to customers, beneficial owners of customers, and the beneficiaries of customers' transactions.
2. risk factors related to countries and geographic areas.
3. risk factors related to products and services provided by the financial institutions or DNFBPs, the transactions and the delivery channels.
4. risk factors related to the purpose for which the customer opened the account or established the business relationship.

5. risk factors related to the level of deposits and the volume of the transactions and operations.
6. risk factors related to the duration of the business relationship with the customer and the frequency of operations.

Article (5)

Financial Institutions and DNFBPs shall identify and assess money laundering and terrorism financing risks that may arise in relation to the development of new products and new business practices, including the new delivery mechanisms to provide services, products or transactions; or the risks arising from the use of new or developing technologies for both new and pre-existing products, prior to the launch or use of such products, practices and technologies. Financial Institutions and DNFBPs shall take appropriate measures to manage and mitigate the risks.

Article (6)

Financial institutions and DNFBPs shall establish programs against money laundering and terrorism financing, which have regard to the risks and the size of the business, and which include the following policies, procedures and controls:

1. appropriate compliance management arrangements, including the appointment of a compliance officer at the management level.
2. appropriate screening procedures to ensure high standards when hiring employees.
3. an ongoing employee-training program.
4. an independent audit unit to test the AML/CFT system.

Article (7)

Financial groups and DNFBPs shall, when implementing programs against ML/TF to all their branches and majority-owned subsidiaries, include in such programs, along with the procedures stipulated in the previous Article, the following:

1. policies and procedures for sharing information required for the purposes of Customer Due Diligence and ML/TF risk management.
2. provision, at group-level compliance, audit and AML/CFT functions, of customer, account and transaction information from branches and subsidiaries, when necessary for AML/CFT purposes. This shall include information and analysis of transactions and activities which appear unusual or suspicious, suspicious transactions reports and underlying

information, or any information which may be necessary to submit a suspicious transaction report.

3. provision of the above mentioned information to branches and subsidiaries, when necessary and appropriate to risk management.
4. adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

Article (8)

1. Financial groups, financial institutions and DNFBPs shall ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the requirements of the State, where the minimum AML/CFT requirements of the host State are less strict than those applied in the State, to the extent that host State laws and regulations permit.
2. If the host State does not permit the proper implementation of AML/CFT measures consistent with the requirements of the State, financial groups, financial institutions and DNFBPs shall apply to their foreign branches and majority-owned subsidiaries appropriate additional measures to manage ML/TF risks, and shall inform their competent supervisory authority.
3. If the additional measures are not sufficient, the competent authorities in the State shall consider applying further supervisory measures, including imposing additional controls on the financial groups, financial institutions, and DNFBPs and, if necessary, suspending their transactions in the host State.

Article (9)

When applying CDD requirements to existing customers, as stipulated in Articles (10) and (11) of the Law, financial institutions and DNFBPs shall take into consideration the materiality and risk of customers. Such measures shall be applied to existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

Article (10)

CDD measures shall be applied, when financial institutions and DNFBPs conduct occasional transactions equal to or exceeding (QR 50.000) fifty thousand Qatari Riyals.

Financial institutions and DNFBPs shall take appropriate measures to identify transactions carried out in several operations involving smaller amounts totaling the designated threshold stipulated above.

Real estate agents shall perform CDD on both the purchaser and the vendor of the property.

Article (11)

Dealers in precious metals or precious stones shall be subject to obligations under the Law whenever they participate in cash transactions equal to or exceeding (QR 50,000) fifty thousand Qatari Riyals.

Article (12)

In cases where financial institutions and DNFBPs form a suspicion of money laundering or terrorism financing when establishing a business relationship with the customer, or throughout the course of that relationship, or when carrying out occasional transactions, they shall:

1. Identify and verify the identity of the customer and the beneficial owner, whether the customer was permanent or occasional, regardless of any exemption or any applicable threshold.
2. Submit a suspicious transaction report to the Financial Information Unit.

Article (13)

Financial institutions and DNFBPs shall identify and verify the identity of the customer, using reliable, independent source documents, data or information, and shall at least obtain the following information:

1. For customers that are natural persons: name of the customer as registered in the official documentation, residence address or domestic address, date and place of birth, and nationality.
2. For customers that are legal persons or legal arrangements: name, legal form and proof of existence of the customer; the regulations and powers that regulate the legal person or arrangement, as well as the names of the relevant persons having a senior management position in the legal person or arrangement; the address of the registered office and, if different, the principal place of business.

For customers that are legal persons or legal arrangements, financial institutions and DNFBPs shall understand the customer's ownership and

control structure; and shall verify the identity of beneficial owners in accordance with Articles (15) and (17) of this Implementing Regulations.

Financial institutions and DNFBPs shall obtain and verify any additional information, as per the level of risks associated with any particular customer.

For all customers, financial institutions and DNFBPs shall:

1. Understand the nature of the customer's business or activity pattern.
2. Verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person, as stipulated in (1 and 2) in the first paragraph of this Article.
3. Understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.
4. Conduct ongoing due diligence on the business relationship, including:

a. scrutinising transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the financial institution's knowledge of the customers, their business and risk profile, including where necessary, the source of funds.

b. ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers.

Article (14)

Financial institutions and DNFBPs shall, in cases where their supervisory authority permit the establishment of a business relationship with a customer prior to verification, adopt risk management procedures concerning the conditions under which a customer may utilise the business relationship.

Article (15)

For customers that are legal persons, financial institutions and DNFBPs shall identifiy and take reasonable measures to verify the identity of the beneficial owner, using relevant information or reliable sources data as follows:

1. Identifying the natural person(s) who ultimately has an effective controlling ownership interest not less than 20% of a legal person or voting rights, and taking reasonable measures to verify the identity of such persons.

2. In case no beneficial owner is identified, or there is a doubt as whether the natural person(s) with controlling ownership interest(s) is the beneficial owner(s) under item (1) above, or where no natural person exerts control

through ownership interests, financial institutions and DNFBPs shall identify the natural person(s) exercising de facto or legal control in the legal person and arrangement through any means, whether directly or indirectly, over the executives, the general assembly, or the operations of the legal person, or any other control instruments.

3. In case no natural person is identified under (1) and (2) above, financial institutions and DNFBPs shall identify and verify the identity of the relevant natural person who holds the position of senior managing official in the legal person.

In cases where financial institutions and DNFBPs are unable to identify at least one natural person who meets the requirements of this Article, they shall not commence a business relationship with the customer, or perform a transaction or continue the relationship, and shall terminate such relationship (for existing customers) and file a suspicious transactions report with the Unit.

Article (16)

Where the customer or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements which ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies. The relevant identification data may be obtained from a public register, from the customer or from other reliable sources.

Article (17)

For customers that are trusts, financial institutions and DNFBPs shall take reasonable measures to identify and verify the identity of the beneficial owners by identifying the settlor, the trustee and the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising, directly or indirectly, ultimate effective control over the trust.

For other types of legal arrangements, the identity of the natural persons in equivalent or similar positions.

Financial institutions and DNFBPs shall take the necessary procedures to determine whether a customer is acting as a trustee of a trust, or holds an equivalent or similar position in other types of legal arrangements.

Article (18)

In addition to the CDD measures required for the customers as set out in the Law and this Implementing Regulations, financial institutions shall conduct the following additional CDD measures on the beneficiaries of life insurance and other investment related insurance policies, as soon as the beneficiaries are identified or designated:

1. For a beneficiary that is identified as specifically named natural or legal person or legal arrangement: taking the name of the person.
2. For a beneficiary that is designated by characteristics or by class, or by other means: obtaining sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout.
3. For both the above cases, verifying the identity of the beneficiary at the time of the payout.

In cases where financial institutions are unable to take the measures mentioned above, they shall file a suspicious transactions report with the Unit.

Article (19)

Financial institutions shall include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable.

If the financial institution determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, it shall perform enhanced due diligence, which should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary of a life insurance policy, at the time of the payout.

Article (20)

Financial institutions and DNFBPs, when relying on third-party financial institutions and DNFBPs to perform the CDD measures as set out in the Law and this Implementing Regulations, shall:

1. Obtain immediately the necessary information concerning the mentioned CDD measures.
2. Ensure that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay.
3. Ensure that the third party is regulated and supervised or monitored, and has measures in place for compliance with CDD and record-keeping

requirements, in accordance with the Law and this Implementing Regulations.

4. Take into consideration the information available on the level of ML/TF risks in countries where are the third parties based.

Article (21)

When financial institutions and DNFBPs rely on a third party that is part of the same financial group, the supervisory authorities, whether in the State or the host State, may determine that the requirements set out in the above Article are met in the following circumstances:

1. the group applies CDD, record-keeping requirements, and AML/CFT programs in line with the Law and this Implementing Regulations.
2. the implementation of these requirements and programs is supervised by a competent authority.
3. any higher country risk is adequately mitigated by the group's AML/CFT policies.

Article (22)

Financial institutions and DNFBPs shall apply enhanced due diligence measures proportionate to the risks, to business relationships and transactions with customers, including financial institutions and DNFBPs from countries for which this iscalled for to do so by the FATF and shall be published by the Committee on its website.

Article (23)

Financial institutions and DNFBPs shall take other measures, pursuant to Article (13) of the Law, that include countermeasures proportionate to the degree of risks specified in the circulars required by the supervisory authorities, based on the data provided by the FATF or in accordance with the measures required by the Committee independently of any call by the FATF to do so.

Article (24)

The Committee shall issue circulars on the vulnerabilities of AML/CFT systems in other countries.

The Committee shall communicate such circulars to the supervisory authorities and the competent authorities, and publish them on its website.

The supervisory authorities shall communicate such circulars to the financial institutions and DNFBPs under their supervision.

Article (25)

Financial institutions and DNFBPs shall verify, to the extent possible and on a reasonable basis, the background and the purpose of all complex or unusual transactions, and all unusual patterns of transactions, which have no apparent economic or clear legal purpose.

Where the ML/TF risks are higher, financial institutions and DNFBPs shall perform enhanced due diligence measures consistent with the risks identified, and shall particularly conduct enhanced ongoing monitoring of the business relationship, to identify unusual or suspicious activities or transactions. The enhanced due diligence measures shall specifically include:

1. Obtaining additional information with respect to the customer, including but not limited to, occupation, volume of assets, information available through public databases and open sources; and regularly updating the identification data of the customer and beneficial owner.
2. Obtaining additional information on the intended nature of the business relationship.
3. Obtaining information on the source of funds or the source of wealth of the customer.
4. Obtaining information on the reasons for intended or performed transactions.
5. Obtaining the approval of senior management to commence or continue the business relationship.
6. Conducting enhanced monitoring of the business relationship, by increasing the number and timings of controls applied, and selecting patterns of transactions that require further examination and verification.
7. Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Article (26)

Where the risks of money laundering or terrorisn financing are lower, financial institutions and DNFBPs may, as specified by the supervisory authority, conduct simplified CDD measures that take into account the nature of these risks, and that are commensurate with the lower risk factors as follows:

1. Verifying the identity of the customer and the beneficial owner after the establishment of the businesss relationship, e.g if account transactions exceed the designated monetary threshold.
2. Reducing the frequency of customer identification updates.
3. Reducing the degree of ongoing due diligence, monitoring and scrutinising transactions, based on a reasonable designated monetary threshold.
4. Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

Simplified CDD measures may relate only to customer acceptance measures or to aspects of ongoing monitoring; and shall not be applied whenever there is suspicion of money laundering or terrorism financing, or where specific higher-risk scenarios apply.

Article (27)

Financial institutions and DNFBPs shall develop appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person, or a family member or close associate of such PEP, and shall take the following additional due diligence measures in relation to them:

1. Obtaining senior management approval for establishing, or continuing for existing customers, such business relationships.
2. Taking reasonable measures to establish the source of wealth and source of funds of customers and beneficial owners of customers identified as politically exposed persons, or family members or close associates of such PEPs.
3. Conduct enhanced ongoing monitoring of the business relationship.

Article (28)

Family members of a politically exposed person shall include any natural person relative by blood or marriage up to the second degree.

Close associates of a politically exposed person shall include any natural person who is a partner in a legal person or legal arrangement, or a beneficial owner of a legal person or arrangement owned or effectively controlled by a politically exposed person, or any person associated with the politically exposed person through a close business or social relationship.

Article (29)

Before making a payout under a life insurance policy, financial institutions shall take reasonable measures to determine whether the beneficiary or the beneficial owner of the beneficiary of a life insurance policy is a politically exposed person.

Where higher risks are identified, financial institutions shall inform senior management before the payout of the policy proceeds, conduct enhanced scrutiny on the whole business relationship with the policyholder, and submit a suspicious transaction report to the Financial Information Unit.

Article (30)

Financial institutions, when establishing a cross-border correspondent relationship or any other similar relationship, shall:

1. Gather sufficient information about the respondent institution to fully understand the nature of the respondent's business, and determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a ML/TF investigation or supervisory action.
2. Assess the respondent institution's AML/CFT controls.
3. Obtain approval from senior management before establishing new correspondent relationship.
4. Clearly understand the respective AML/CFT responsibilities of each institution.

Article (31)

With respect to "payable through accounts", financial institutions shall satisfy themselves that the respondent bank:

1. has performed CDD obligations as required by the Law and this Implementing Regulations on its customers that have direct access to the accounts of the correspondent bank; and
2. is able to provide relevant CDD information upon request to the correspondent bank.

Article (32)

When conducting wire transfers, ordering financial institutions shall :

1. Obtain and verify information related to the originator and the beneficiary, when conducting wire transfers equal to, or exceeding (QR 3.500) three thousand five hundred Qatari Riyals, and ensure that it includes the following:

a. The full name of the originator and the beneficiary.
b. The originator and the beneficiary account number or, in the absence of an account, a unique transaction reference number, which permits traceability of the transaction.
c. The originator's address, or national identity number, or customer identification number, or date and place of birth. Such information shall be included in the message or payment form accompanying the transfer.

2. Whenever the information referred to in paragraph (1) above is available to the beneficiary financial institution and competent authorities by other means, the financial institution may only include the account number or the unique transaction reference number in the information accompanying the domestic wire transfer, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary, within three (3) business days of receiving the request either from the beneficiary financial institution or from competent authorities. The Public Prosecutor may compel immediate production of such information.
3. Ensure that cross-border wire transfers of a value below the threshold specified in paragraph (1), include the name of the originator and the beneficiary, and both the originator and the beneficiary account numbers or a unique transaction reference number which permits traceability of the transaction. In such case, the ordering financial institution is not required to verify the information, unless there is suspicion of ML/TF.
4. Ensure, where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, that the batch file contains required and accurate originator information and full beneficiary information, that is fully traceable within the beneficiary country; and shall include the originator's account number or unique transaction reference number.
5. Not execute the wire transfer if it does not comply with the requirements specified in this Article.

Article (33)

Intermediary financial institutions, when conducting cross-border wire transfers, shall:

1. Ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it.

2. Take reasonable measures, which are consistent with straight-through processing, to identify the wire transfers that lack required originator or beneficiary information.

Article (34)

Beneficiary financial institution shall take reasonable measures to identify cross-border wire transfers that lack required originator or beneficiary information, which may include post-event monitoring or real-time monitoring, where feasible.

For cross-border wire transfers of more than (QR 3.500) three thousand five hundred Qatari Riyals, the beneficiary financial institution shall verify the identify of the beneficiary, if the identity has not been previouly verified, and maintain the information collected in the course of verification in accordance with the requirements stipulated in the Law.

Article (35)

Ordering, intermediary, and beneficiary financial institutions involved in a wire transfer shall maintain all originator and beneficiary information, including the originator's account number or unique transaction reference number, for at least (10) ten years following completion of the transaction.

Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary financial institution shall maintain, for at least (10) ten years, all the information received from the ordering financial institution or another intermediary financial institution.

Article (36)

Intermediary and beneficiary financial institutions shall establish effective risk-based policies and procedures for determining when to execute, reject, or suspend wire transfers lacking required originator or beneficiary information; and the appropriate follow-up actions.

Article (37)

MVTS providers shall:

1. Comply with all the relevant requirements of the Law and this Implementing Regulations, whether they operate directly or through their agents.

2. Maintain a current list of their agents accessible by the relevant competent authority.
3. Include their agents in their AML/CFT programs and monitor them for compliance with these programs.

Article (38)

In the case of a MVTS provider that controls both the ordering and the beneficiary sides of a wire transfer, the MVTS provider shall:

1. Take into account all the information from both the ordering and beneficiary sides to determine whether an STR has to be filed.
2. File an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Information Unit.

Article (39)

Financial institutions and DNFBPs shall report suspicious transactions in the form specified by the Unit, and in line with its published instructions and guidance.

Article (40)

Where lawyers, notaries, accountants and legal accoutants seek to dissuade a client from engaging in illegal activity, this does not amount to tipping-off as stipulated in Article (22/second paragraph) of the Law .

Chapter 3

Declaration to Customs

Article (41)

Any natural person entering or leaving the State, and is in the possession of currencies, bearer negotiable instruments, or precious metals or stones; or arranging for the transportation thereof into or outside the State, through a person, mail, cargo or any other means, shall make a declaration of value to the competent customs officer, when that value is equal to or exceeds (QR 50,000) fifty thousand Qatari Riyals, and shall fill out the relevant customs declaration form.

Article (42)

Any legal person exporting or importing a cargo of currencies, bearer negotiable instruments, or precious metals or stones of a value equal to or exceeding (QR 50,000) fifty thousand Qatari Riyals, shall make a declaration of value, fill out the relevant customs declaration form, and obtain necessary approvals from the competent authorities.

Article (43)

All NPOs willing to transport currencies, bearer negotiable instruments, precious metals or stones of a value equal to or exceeding (QR 50,000) fifty thousand Qatari Riyals, shall make a declaration of value and fill out the relevant customs declaration form, after submitting an evidence of consent from the Regulatory Authority for Charitable Activities under the provisions of the Law regulating charitable activities.

Article (44)

Upon false declaration or a failure to declare the value of currencies or bearer negotiable instruments or precious metals or stones that is equal to or exceeding (QR 50,000) fifty thousand Qatari Riyals, the competent customs officer may take the following measures:

1. Seize all currencies, bearer negotiable instruments, or precious metals or stones.
2. Draft an incident report.
3. Request the carrier to provide additional information with regard to the origin of the currencies, bearer negotiable instruments, or precious metals or stones and the purpose of their transportation.

The customs officer may arrest the individuals involved in the transportation of the currencies, bearer negotiable instruments, or precious metals or stones, and shall immediately surrender them to the competent security department within the Ministry of Interior and refer the incident report and the seized items to the Public Prosecution to take the relevant necessary procedures.

Article (45)

Upon false declaration or a failure by the importer or exporter to declare the value of the cargo of currencies or bearer negotiable instruments or precious metals or stones that is equal to or exceeding (QR 50,000) fifty thousand Qatari Riyals, the customs officer may take the following measures:

1. Seize the cargo of currencies, bearer negotiable instruments, or precious metals or stones.
2. Draft an incident report.
3. Request the importer, or the exporter, or the legal person, or the NPO, or their legal representative to provide additional information on the reasons for failing to declare or for making false declaration.

The customs officer may arrest the individuals involved in the transportation of the currencies, bearer negotiable instruments, or precious metals or stones and shall surrender them to the competent security department within the Ministry of Interior and refer the incident report and the seized items to the Public Prosecution to take the relevant necessary procedures.

Article (46)

The customs authorities shall communicate to the Unit, any suspicions that the the transportation of currencies, bearer negotiable instruments, or precious metals or stones, is related to ML/TF or predicate offences; or when the carrier makes false declaration or fails to declare.

Article (47)

The customs authorities shall collect data and information on the movement of currencies, bearer negotiable instruments, or precious metals or stones. To that end, customs authorities shall exercise the following powers:

1. Collecting declaration forms with regard to the value of the currencies, bearer negotiable instruments, or precious metals or stones in possession of persons entering or exiting the State.

2. Validating the information provided in the declaration forms.
3. Verifying that the currencies and bearer negotiable instruments are not counterfeited.
4. Verifying that currencies can be circulated pursuant to the laws regulating their issuance.
5. If precious metals and stones in the possesion of persons entering or exsting the State are for commercial purposes, the customs authorities shall ascertain their value through the purchase invoice.
6. Entering the information obtained from such declarations in a database by the customs officer and making it accessible by the Unit.
7. Maintaining documents and data pertaining to the declared or detected currencies, bearer negotiable instruments, or precious metals or stones and the identification data of the bearers, for at least ten (10) years, in the following cases:
   a. when a declaration equivalent to, or exceeding (QR 50,000) fifty thousand Qatari Riyals is made.
   b. there is a false declaration.
   c. there is a suspicion of ML/TF.
8. Maintaining and disseminating statistics on the amount of incoming and outgoing cross border currencies, bearer negotiable instruments, or precious metals or stones, and on the false declarations; and on the disposition of such currencies, bearer negotiable instruments, or precious metals or stones by the customs authorities, as well as any other statistics requested by the Committee.
9. Exchanging information on the value of the declared or detected currencies, bearer negotiable instruments or precious metals or stones, and the identification data of the bearers, with the competent domestic authorities. Such information can be exchanged with competent international authorities subject to the principle of reciprocity or pursuant to the international agreements.
10. Cooperating and coordinating with the competent authorities for the purposes of implementing this Article.

Article (48)

The customs authorities shall issue decisions, directives and guidelines for implementing the provisions of Chapter 4 of the Law.

Chapter 4

National Anti-Money Laundering and Terrorism Financing Committee

Article (49)

The Committee shall maintain a database of all information received from the national authorities, in relation to matters related to their scope of work. The database shall contain ML/TF-related statistics, including suspicious transactions reports received and disseminated, investigations, prosecutions, and convictions related to money laundering and terrorism financing; frozen, seized and confiscated properties, requests for mutual legal assistance and other requests for international cooperation.

Article (50)

The Committee shall:

1. Ensure that the National Risk Assessment covers all relevant sectors, including financial institutions, DNFBPs, NPOs, cross-border transportation of cash, in addition to the activities of law enforcement authorities; apply a risk-based approach to allocate resources and implement measures to prevent or mitigate ML/TF.
2. Send the National Risk Assessment Report to the Governor to be submitted to the Council of Ministers for approval. The Committee shall communicate the outcomes of the assessment to the AML/CFT national authorities to include them in their action plans for implementation.
3. Oversee the update of the National Risk Assessment at least once each (3) three years, and when necessary.
4. Coordinate with the supervisory authorities to communicate the outcomes of the National Risk Assessment to the entities under their supervision, and ensure that risks are addressed pursuant to the National Strategy of combating money laundering, terrorism financing and the financing of proliferation of weapons of mass destruction.
5. Coordinate with the competent authorities to raise awareness about ML/TF risks; and with supervisory authorities to ensure that financial institutions and DNFBPs are capable of countering money laundering, predicate offences and terrorism financing.

Article (51)

The Committee shall work with the supervisory authorities to identify and assess ML/TF risks that may arise in relation to the development of new products and

new business practices, including the use of delivery channels, or the development of new technologies for new and pre-existing products.

Chapter 5

Financial Information Unit

Article (52)

The Unit shall create and adopt forms and procedures for requesting and disseminating information, suspicious transaction reports, and other relevant reports and respective timelines in coordination with the competent authorities, in order to access financial, administrative and law enforcement information maintained by the national competent authorities, as well as the relevant information collected or obtained by other authorities, or collected or obtained on behalf of other authorities.

The Unit may use publically available information and commercially held databases.

Article (53)

The Unit shall take the necessary measures to protect and access the information available in its database, or any accessible or obtainable information, provided that these measures shall be, at a minimum, in conformity with the Egmont Group standards on exchanging information with counterpart Financial Information Units, and with any international standards that, are or may be, applicable at the national level. To this effect, the Unit shall:

1. Set rules governing the security, confidentiality and privacy of information through the processing, dissemination, protection of, and access to, information.
2. Ensure that QFIU employees have the necessary security clearance levels and understand their responsibilities in handling and disseminating (sensitive and confidential) information.
3. Ensure that there is limited access to the Unit's facilities and information, including information technology systems.
4. Use dedicated, secure and protected channels for the dissemination of information to national and international competent authorities.

Article (54)

The Unit shall maintain in its database any available information on suspicious transactions, suspects and all data related to money laundering, terrorism financing and predicate offences.

The competent authorities shall commit to inform the Unit of the available information that they maintain in regards to money laundering, predicate offences or terrorism financing; actions taken and results thereof, where such actions and results are related to measures required or adopted by the Unit.

Article (55)

The Unit, upon receiving suspicious transaction reports from financial institutions and DNFBPs or information related to money laundering, predicate offences, or terrorism financing , shall particularly conduct:

1. Operational analysis: by using available and obtainable information to identify specific targets, follow the trail of particular activities or transactions and determine links between those targets and possible proceeds of crime, money laundering, predicate offences or terrorism financing.
2. Strategic analysis: by using available and obtainable information, including data that may be provided by other competent authorities, to identify money laundering and terrorism financing related trends and patterns.

Article (56)

The Unit shall:

1. Identify the requirements for collecting and analysing the information received from financial institutions and DNFBPs.
2. Approve the reporting requirements for financial institutions and DNFBPs, and the relevant forms and procedures, in coordination with the supervisory authorities and competent authorities.
3. Approve forms and procedures relating to requesting information from the reporting entities, in coordination with the supervisory authorities.
4. Notify the relevant supervisory authority when a financial institution or DNFBP fails to abide by the obligations provided for in this Article.

Article (57)

The Unit shall exchange information and cooperate with the competent authorities and supervisory authorities, as follows:

1. The Unit shall spontaneously disseminate any information or results of analysis undertaken whenever there are grounds to believe that such information is useful in identifying proceeds of crime or terrorism financing. The Unit may decide the information to be disseminated.

2. The Unit may decide, at its own discretion, to provide information upon request.
3. The Unit shall set forth mechanisms and procedures to enable competent authorities to request information; and to respond to urgent requests for information.

Article (58)

The Unit shall maintain statistics on received and disseminated suspicious transaction reports, international cooperation and other matters requested by the Committee.

Chapter 6

Supervisory Authorities

Article (59)

The following supervisory authorities shall supervise and monitor the corresponding sectors under their supervision, and ensure their compliance with AML/CFT requirements:

	The supervisory authority	The Sector
1	**Qatar Central Bank**	- Banks and exchange houses. - MVTS providers. - insurance and reinsurance. - finance and investment companies.
2	**Qatar Financial Markets Authority**	- financial brokerage firms/intermediaries. - Qatar Stock Exchange. - Qatar Central Securities Depository.
3	**Ministry of Justice**	- Lawyers. - Notaries. - real estate agents
4	**Ministry of Commerce and Industry**	- legal accountants. - traders in precious metals and stones. - trust and company service providers.
5	**Qatar Financial Centre Regulatory Authority**	- financial institutions and DNFBPs established in the Qatar Financial Centre.
6	**The Regulatory Authority for Charitable Activities**	- Non-Profit Organizations (NPOs).

The supervisory authorities shall include any other competent authority empowered by law to regulate, supervise or monitor the financial institutions and DNFBPs or NPOs.

Article (60)

Supervisory authorities shall:

1. Monitor and inspect financial institutions, DNFBPs and NPOs to ensure their compliance with the requirements of the Law and this Implementing Regulations. The supervisory authorities may obtain any information they may request in accordance with the provisions of Article (41) of the Law.
2. Issue instructions, rules, guidelines or recommendations, or any other instruments pursuant to the provisions of the Law, this Implementing Regulations and any other provisions, for combatting money laundering and terrorism financing purposes. Provide guidance and feedback to the entities under their supervision on the compliance with the requirements of the Law, the Implementing Regulations and the instruments issued by the supervisory authorities; and on enhancing the effectiveness and efficiency of applicable policies and procedures.
3. Assist the Unit to develop reporting procedures for supervised entities, in line with the relevant national and international standards. The supervisory authorities shall communicate to the Unit and the Public Prosecutor, any information identified while exercising their powers that could be related to money laundering, terrorism financing, and predicate offences.
4. Cooperate and exchange information with competent authorities related to detecting and reporting money laundering, predicate offences and terrorism financing.

Article (61)

Supervisory authorities shall, in performing their supervisory powers over financial institutions, DNFBPs and NPOs, apply a risk-based approach to ensure that financial institutions, DNFBPs and NPOs implement AML/CFT measures, and identify the level and focus of supervision required for each supervised entity. The supervisory authorities shall particularly:

1. Ensure that entities under their supervision have necessary systems in place to ensure and monitor compliance with their AML/CFT obligations under the Law.
2. Ensure that the entities under their supervision, their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the State's requirements, where the minimum AML/CFT requirements of the host country are less strict than those of the State, to the extent that host country laws and regulations permit.

The supervisory authorities, in performing their supervisory powers over financial institutions pursuant to the Law, shall take into consideration the following:

1. For core principles financial institutions, regulation and supervision shall be in line with the core principles, where relevant for AML/CFT, including the application of consolidated group supervision for AML/CFT purposes.
2. For all other financial institutions, regulation and supervision or monitoring shall have regard to the ML/TF risk level in that sector.

Article (62)

Supervisory authorities shall determine the frequency and intensity of AML/CFT supervision on the basis of:

1. The ML/TF risks and the understanding of such risks, internal controls, policies and procedures associated with the institution or group and their adequacy, as identified by the supervisory authority assessment of the institution's or group's risk profile.
2. The ML/TF risks present in the State.
3. The diversity and number of financial institutions, DNFBPs and NPOs in the State, and the degree of discretion allowed to them under the risk-based approach.

Article (63)

Supervisory authorities shall:

1. Ensure that the financial institutions and DNFBPs conduct their risk assessment, review their ML/TF risk profile and characteristics, and analyse the results of such reviews to identify challenges of compliance with the AML/CFT standards.
   They shall regularly review the ML/TF risk assessment related to financial institutions, DNFBPs, and when there are major changes in the management and operations thereof.
2. Provide proposals to enhance the effectiveness and adequacy of the existing procedures and policies.
3. Use the outcomes of the risk assessment to appoint supervisors, allocate their supervision and determine the means and degree of inspection.

Supervisory authorities shall also maintain and submit statistics to the Committee concerning the measures adopted and sanctions imposed by virtue

of the Law; the international cooperation; and any other matters required by the Committee.

Article (64)

Petitions against decisions referred to in Article (44) of the Law may be filed with the relevant supervisory authority within (15) fifteen days from the petitioner being notified in writing of the decision issued against him, or of his knowledge thereof.

The petition shall include:

1. The petitioner's full name, title, capacity and address.
2. The appealed decision, the date of its issuance, and the date of notification of the petitioner or his knowledge thereof.
3. The grounds for petition, the supporting documents and briefs.
4. The petitioner's specific requests.
5. The means appropriate for the petitioner to receive notifications, whether by fax, e-mail, telephone or any other means.

Article (65)

The supervisory authority shall notify the petitioner of the hearing and all related papers, by any of the means specified above.

If the petitioner did not present himself or his representative, he shall be notified of another date. If he fails to attend, the petition shall be decided in his absence.

In all cases, the relevant supervisory authority shall decide on the petition, within a period not exceeding (30) thirty days from the date of lodging the petition.

The decision of the relevant supervisory authority in this regard shall include a summary of the petition and the based on reasons. The petitioner shall be notified of such decision in writing, within (7) seven days of its issuance, by the means of notification specified in the petition lodged.

Chapter 7

International Cooperation

Section One

Mutual Legal Assistance

Article (66)

When a mutual legal assistance request is related to a confiscation order or the execution thereof, the Court shall consider this request, at the motion of the Public Prosecutor and pursuant to the provisions of Article (68) of the Law.

Article (67)

Having regard to any bilateral or multilateral agreements to which the State is party, or to any arrangements or memoranda of understanding in regard to sharing confiscated property with foreign countries, the Public Prosecutor may decide to share a part of the confiscated funds.

Section Two

Cooperation between the Unit and its Foreign Counterparts

Article (68)

The Unit shall, spontaneously or upon request, provide the widest range of cooperation to foreign counterparts, according to the rules of bilateral or multilateral agreements to which the Unit is party, including cooperation with counterpart Egmont members. The Unit shall also provide cooperation according to the arrangements or memoranda of understanding signed with its foreign counterparts, or to the principle of reciprocity, regardless of the operating model of its counterparts and the status thereof.

Article (69)

The Unit may request information from counterpart Financial Information Units. In such cases, the Unit shall provide all relevant information in its possession, including a description of the case under analysis and potential links to the State receiving the request for information.

The Unit may exchange with its foreign counterparts all information received or collected according to the provisions of Chapter (6) of the Law, and any other

information obtainable and accessible by the Unit, directly or indirectly, from domestic sources.

The Unit shall provide feedback to its foreign counterparts, upon request, regarding the use of information received and the results of the ensuing analysis.

Section Three

Cooperation between Supervisory Authorities of Financial Institutions and their Foreign Counterparts

Article (70)

Supervisory authorities of financial institutions shall, spontaneously or upon request, provide the widest range of international cooperation related to supervision for AML/CFT purposes to foreign counterparts according to the rules of bilateral or multilateral agreements to which they are party, or to the arrangements or memoranda of understanding signed with foreign counterparts, or to the principle of reciprocity, regardless of the respective nature or status of the foreign counterpart, and pursuant to the applicable international standards for supervision.

Article (71)

Supervisory authorities of financial institutions may exchange with their foreign counterparts all information domestically available to them, including information held by financial institutions under their supervision, in a manner proportionate to their respective needs.

Article (72)

Supervisory authorities of financial institutions shall exchange with their foreign counterparts, in particular with supervisory authorities that have a shared responsibility for financial institutions operating in the same financial group, relevant information for AML/CFT purposes, including:

1. Domestic legislative and regulatory system and general information on the financial sectors.
2. Prudential information, such as information on the financial institution's business activities, beneficial ownership, management, and fit and properness standards.
3. AML/CFT information, such as internal AML/CFT procedures and policies of financial institutions, customer due diligence information, customer files, samples of accounts and transaction information.

Article (73)

Supervisory authorities of financial institutions may collect necessary information on behalf of their foreign counterparts, and when necessary assist them in collecting such information themselves, with the purpose of facilitating an effective supervision of the financial institutions operating in the same financial group.

Article (74)

Supervisory authorities of financial institutions shall require the requesting foreign counterparts to have prior authorisation for any dissemination of information exchanged, or for any use of that information for supervisory and non-supervisory purposes,

In cases where the requesting foreign counterpart is under a legal obligation to disclose or report the information, supervisory authorities shall require their foreign counterparts to inform them of such obligation.

Section Four

Cooperation between Law Enforcement Authorities and their Foreign Counterparts

Article (75)

Law enforcement authorities may exchange all domestically available information with their foreign counterparts for conducting inquiries and gathering evidence relating to money laundering, predicate offences and terrorism financing, including information related to the identification and tracing of the proceeds and instrumentalities of crime.

Article (76)

Law enforcement authorities shall use their powers by virtue of the Law and this Implementing Regulations, the Criminal Procedure Code and the laws regulating their duties, to conduct inquiries on behalf of foreign counterparts, and to collect and exchange requested information.

Law enforcement authorities shall be subject to the requirements of chapter (10) of the Law.

Article (77)

The provisions of the preceding two Articles shall apply to all competent authorities entrusted with the powers of judicial commissioners and initiate inquiries and investigations to gather evidence relating to money laundering, terrorism financing and predicate offences. Competent authorities shall include the specialized departments within the Ministry of Interior, the State Security Bureau and the General Authority of Customs.

Section Five

Other Forms of Cooperation

Article (78)

Competent authorities shall use effective means to take expeditious and prompt action in response to requests for information.

Competent authorities shall respond to requests for information pursuant to the enforceable provisions of laws, after ascertaining for what purpose and on whose behalf the request is made, and when necessary verifying the authorization given to the requesting authority.

Article (79)

The competent authority may receive requests for information indirectly from a foreign non-counterpart authority, provided that the requesting authority makes it clear for what purpose and on whose behalf the request is made.

The request for information shall be indirect when the required information is sent to the requesting authority through a competent authority in the State or a competent authority in one or more foreign countries, provided that a prior authorization or mandate is obtained for such an exchange of information.

****