هيئة تنظيم مركز قطر للمال
QATAR FINANCIAL CENTRE
REGULATORY AUTHORITY

Summary of changes to QFC Regulatory Rules: AML/CFT Rules 2020

At the end of 2019, the Regulatory Authority completed its assessment of new State of Qatar AML/CFT legislation, which included the following:

- Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing (AML/CFT Law);

- Decision No. (41) of 2019 Promulgating the Implementing Regulations of Law No. (20) of 2019 on Combatting Money Laundering and Terrorism Financing (IRs); and

- Law No. (27) of 2019 Promulgating the Law on Combating Terrorism (CT Law).

As a result of its assessment, the Regulatory Authority made a range of limited rule amendments to its AML/CFT Rules framework. The amendments to the Rules were introduced by the Anti-Money Laundering and Combating the Financing of Terrorism Rules 2019 and Anti-Money Laundering and Combating the Financing of Terrorism (General Insurance) Rules 2019, which came into force on 1 February 2020.

It should be noted that the amendments have not resulted in any substantial change to the content or structure of the previously in force AML/CFT Rules.

The next section of this note sets out a summary of the rule amendments. While the summary is intended to assist firms' understanding of the recent rule changes, firms should not place sole reliance on the summary as an analysis of the changes to their obligations, and should conduct their own analysis. Firms remain responsible for ensuring that their policies, procedures, systems, and controls (PPSC) are in compliance with the AML/CFTR or AMLG, as applicable.

AML/CFTR

Section 1: Definitions

The Definitions section of the Rules have been revised to take account of new definitions contained in the AML/CFT Law, the IRs and CT Law. The following key definitions have been amended or introduced, and revisions are highlighted in yellow:

Politically exposed persons

- **Previous** – PEP means a politically exposed person.

Note Politically exposed person is defined in r 1.3.6.

1.3.6 **Who is a *politically exposed person*?**

(1) A ***politically exposed person*** (***PEP***) is—

(a) an individual (***A***) who is, or has been, entrusted with prominent public functions in a foreign jurisdiction; or

(b) a family member of A; or

(c) a close associate of A.

(2) In deciding whether a person is a close associate of A, a firm need only have regard to information that is in its possession or is publicly known.

(3) Without limiting subrule (1) (a), individuals ***entrusted with prominent public functions*** include the following:

(a) heads of state, heads of government, ministers and deputy or assistant ministers;

(b) members of parliament, other senior politicians and important political party officials;

(c) members of supreme courts, of constitutional courts, or of other high-level judicial bodies whose decisions are not generally subject to further appeal, other than in exceptional circumstances;

(d) members of the boards of central banks;

(e) ambassadors and chargés d'affaires;

(f) high-ranking officers in the armed forces;

(g) members of administrative, management or supervisory bodies of state-owned enterprises (other than members who are middle ranking or more junior officials).

(4) Without limiting subrule (1) (b), ***family members of A*** includes—

(a) each spouse, child and parent of A; and

(b) each spouse, child and parent of each person referred to in paragraph (a).

(4A) In subrule (4)—

child includes an adopted child.

(5) Without limiting subrule (1) (c), close associates of A include the following:

(a) individuals known to have joint beneficial ownership of a legal entity or legal arrangement, or any close business relations, with A;

(b) individuals with sole beneficial ownership of a legal entity or legal arrangement known to have been set up for A's benefit.

- **New** - ***PEP*** means a politically exposed person.

person means:

(a) an individual (including an individual occupying an office from time to time); or

(b) a legal person.

politically exposed person *(or* ***PEP****)* has the meaning given by rule 1.3.6.

1.3.6 **Politically exposed persons, their family members and associates**

(1) A ***politically exposed person (PEP)*** means an individual who is, or has been, entrusted with prominent public functions.

Examples of persons who can be PEPs

1 Heads of State or of government

2 senior politicians

3 senior government, judicial or military officials

4 members of Parliament

5 important political party officials

6 senior executives of state owned companies

7 members of senior management (directors, deputy directors and members of the board or equivalent functions) in international organisations.

(2) A ***family member of a PEP*** means an individual related to the PEP by blood, or by marriage, up to the second degree.

Examples of individuals related to a PEP in the first or second degree

1 the PEP's father and mother

2 the PEP's husband or wife

3 the PEP's father-in-law or mother-in law

4 the PEP's son or daughter

5 the PEP's stepson or stepdaughter

6 the PEP's grandfather and grandmother

7 the PEP's brother or sister

8 the PEP's brother-in-law or sister-in-law

9 the PEP's grandson or granddaughter

(3) A person is a ***close associate of a PEP*** if the person:

(a) is in partnership with the PEP in a legal person or legal arrangement;

(b) is associated with the PEP through a business or social relationship; or

(c) is a beneficial owner of a legal person or legal arrangement owned, or effectively controlled, by the PEP.

Terrorist act

- **Previous** – terrorist act includes—

(a) an act that constitutes an offence within the scope of, and as defined in, any of the following treaties:

(i) the Convention for the Suppression of Unlawful Seizure of Aircraft (1970);

(ii) the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971);

(iii) the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973);

(iv) the International Convention against the Taking of Hostages (1979);

(v) the Convention on the Physical Protection of Nuclear Material (1980);

(vi) the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988);

(vii) the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988);

(viii) the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (1988);

(ix) the International Convention for the Suppression of Terrorist Bombings (1997); and

(b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, if the purpose of the act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.

- **New** - has the same meaning as in the AML/CFT Law, Chapter 1.

Terrorism financing

- **Previous** – terrorist financing means the act of willingly, directly or indirectly, providing or collecting (or attempting to provide or collect)

funds in order to use them to commit a terrorist act, or knowing that the funds will be used in whole or part—

(a) for the execution of a terrorist act; or

(b) by a terrorist or terrorist organisation.

- **New** - has the same meaning as in the AML/CFT Law, Chapter 2, Article (3).

Terrorist organisation

- **Previous** – means any group of terrorists that—

(a) commits, or attempts to commit, a terrorist act by any means, directly or indirectly, unlawfully and wilfully; or

(b) participates as an accomplice in a terrorist act; or

(c) organises or directs others to commit a terrorist act; or

(d) contributes to the commission of a terrorist act by a group of persons acting with a common purpose if the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

- **New** - means a group of terrorists.

Beneficial owner

- **Previous** – has the meaning given by rule 1.3.5.

1.3.5 Who is the *beneficial owner*?

(1) The ***beneficial owner*** is—

(a) for an account—the individual who ultimately owns, or exercises effective control, over the account; or

(b) for a transaction—the individual for whom, or on whose behalf, the transaction is ultimately being, or is ultimately to be, conducted; or

(c) for a legal person or legal arrangement—the individual who ultimately owns, or exercises effective control over, the person or arrangement.

Note ***Account***, ***transaction***, ***legal person*** and ***legal arrangement*** are defined in the glossary.

(2) Without limiting subrule (1) (a), the ***beneficial owner*** for an account includes any individual in accordance with whose instructions any of the following are accustomed to act:

(a) the signatories of the account (or any of them);

(b) any individual who, directly or indirectly, instructs the signatories (or any of them).

(3) Without limiting subrule (1) (c), the ***beneficial owner*** for a corporation includes—

(a) an individual who, directly or indirectly, owns or controls at least 25% of the shares or voting rights of the corporation; and

(b) an individual who, directly or indirectly, otherwise exercises control over the corporation's management.

(4) Without limiting subrule (1) (c), the ***beneficial owner*** for a legal arrangement that administers and distributes funds includes—

(a) if the beneficiaries and their distributions have already been decided—an individual who is to receive at least 25% of the funds of the arrangement; and

(b) if the beneficiaries or their distributions have not already been decided—the class of persons in whose main interest the arrangement is established or operated as beneficial owner; and

(c) an individual who, directly or indirectly, exercises control over at least 25% (by value) of the property of the arrangement.

- **New** -

1.3.5 Who is the *beneficial owner*?

(1) The ***beneficial owner*** is:

(a) for an account—the individual who ultimately owns, or exercises effective control, over the account;

(b) for a transaction—the individual for whom, or on whose behalf, the transaction is ultimately being, or is ultimately to be,

conducted (whether by proxy, trusteeship or mandate, or by any other form of representation); or

(c) for a legal person or legal arrangement—the individual who ultimately owns, or exercises effective control over, the person or arrangement.

(2) Without limiting subrule (1) (a), the ***beneficial owner*** for an account includes any individual in accordance with whose instructions any of the following are accustomed to act:

(a) the signatories of the account (or any of them);

(b) any individual who, directly or indirectly, instructs the signatories (or any of them).

(3) Without limiting subrule (1) (c), the ***beneficial owner*** for a corporation includes:

(a) an individual who, directly or indirectly, owns or controls at least 20% of the shares or voting rights of the corporation; and

(b) an individual who, directly or indirectly, otherwise exercises control over the corporation's management.

(4) Without limiting subrule (1) (c), the ***beneficial owner*** for a legal arrangement that administers and distributes funds includes:

(a) if the beneficiaries and their distributions have already been decided—an individual who is to receive at least 20% of the funds of the arrangement;

(b) if the beneficiaries or their distributions have not already been decided—the class of individuals in whose main interest the arrangement is established or operated as beneficial owner; and

(c) an individual who, directly or indirectly, exercises control over at least 20% (by value) of the property of the arrangement.

Funds

- **Previous** – includes assets of any kind.
  Note Asset is defined in this glossary.

- **New** - funds means assets or properties of every kind (whether physical or non-physical, tangible or intangible or movable or immovable, however acquired, and of any value), including:

(a) financial assets and all related rights;
(b) economic resources such as oil and other natural resources, and all related rights;
(c) legal documents or instruments in any form, including electronic or digital copies, evidencing title to, or share in, such assets or resources;
(d) any interest, dividends or other income on such assets or resources; and
(e) any value accruing from, or generated by, such assets or resources, which could be used to obtain funds, goods or services.

Customer

- **Previous** – customer has the meaning given by rule 1.3.4.

Who is a customer?

A ***customer***, in relation to a person (***A***), includes any person (***B***) who engages in, or who has contact with A with a view to engaging in, any transaction with A or a member of A's group—

(a) on B's own behalf; or
(b) as agent for or on behalf of another person;

and, to remove any doubt, also includes a client or investor, or prospective client or investor, of A or a member of A's group.

Transaction and ***group*** are defined in the glossary.

- **New** - ***customer*** has the meaning given by rule 1.3.4.

Who is a *customer*?

(1) A *customer*, in relation to a firm, includes any person who engages in, or who has contact with the firm with a view to engaging in, any transaction with the firm or a member of the firm's group:
(a) on the person's own behalf; or
(b) as agent for or on behalf of another person.

(2) To remove any doubt, *customer* also includes:
(a) any person receiving a service offered by the firm (or by a member of the firm's group) in the normal course of its business; and
(b) a client or investor, or prospective client or investor, of the firm or a member of the firm's group.

Group

- **Previous** – *group*, in relation to a legal person (*A*), means the following:
  - (a) A;
  - (b) any parent entity of A;
  - (c) any subsidiary (direct or indirect) of any parent entity.

- **New** - ***group***, in relation to a firm, means 2 or more entities consisting of:
  - (a) a parent company or other legal person exercising control, and coordinating functions, over the rest of the group for the application of group supervision; and
  - (b) 1 or more branches or subsidiaries that are subject to AML/CFT policies, procedures systems and controls at group level.

Non-profit organisations

- **Previous** – ***non-profit organisation*** includes an entity (other than an individual) that primarily engages in raising or disbursing funds for—
  - (a) charitable, religious, cultural, educational, social, fraternal or similar purposes; or
  - (b) carrying out other types of charitable or similar acts.

- **New** - ***non-profit organisation*** means a legal person, legal arrangement or other organisation that engages in raising or disbursing funds for:
  - (a) charitable, religious, cultural, educational, social, fraternal or similar purposes; or
  - (b) carrying out other types of charitable works for public benefit.

Proceeds of crime

- **Previous** – ***proceeds of criminal conduct***, in relation to any person who has benefited from criminal conduct, includes that benefit.

- **New** - ***proceeds of crime*** means funds derived or obtained, directly or indirectly, from a predicate offence (within the meaning given by the AML/CFT Law, Chapter 1), including any income, interest, revenue or other product from such funds, whether or not the funds have been converted or transferred, in whole or in part, into other properties or investment yields.

Originator and recipient information

Previous – 3.3.10 Wire transfers, money or value transfer services, etc

(13) In this rule:

full originator information means the following information about the originator:

(a) the originator's name;

(b) the originator's account number or, if there is no account number, a unique reference number;

(c) the originator's address, national identity number, customer identification number, or date and place of birth.

full recipient information means the following information about the beneficiary:

(a) the recipient's name;

(b) the recipient's account number, or if there is no account number, a unique reference number.

threshold amount means 4,000 Riyals (or its equivalent in any other currency at the relevant time).

New - full originator information means:

(a) the originator's name;

(b) the originator's account number or, if there is no account number, a unique reference number (being numbers that are traceable to the originator);

(c) the originator's address, national identity number, customer identification number, or date and place of birth.

full recipient information means the recipient's name and the recipient's account number or, if there is no account number, a unique reference number (being numbers that are traceable to the recipient).

Targeted financial sanction

- **New** - ***targeted financial sanction*** means asset freezing or any prohibition to prevent funds from being made available, directly or indirectly, for the benefit of persons or entities listed in accordance with the Law No. (27) of 2019 on Combating Terrorism.

Note Under the Law on Combating Terrorism, the National Counter Terrorism Committee is responsible for implementing the requirements relating to targeted financial sanctions. For how to implement targeted financial sanctions, see guidelines under that Law.

National risk assessment

- **New** - ***National Risk Assessment*** means the series of activities prepared and supervised by the NAMLC to identify and analyse the threats faced by Qatar and its financial system from money laundering, terrorism financing, and the financing of the proliferation of weapons of mass destruction.

Section 2: Effective risk-based approach

Amendments to elements of the requirement that firms implement an effective risk-based approach to AML/CFT, key changes include the following:

I. **Part 1.2 – Rule 1.2.1 – Principle 1 – responsibilities**

Previous –

1.2.1 Principle 1—senior management responsibility
The senior management of a firm must ensure that the firm's policies, procedures, systems and controls appropriately and adequately address the requirements of the AML/CFT Law and these rules.

New –

1.2.1 Principle 1—responsibilities
The Governing Body of a firm is responsible for approving the policies, procedures, systems and controls necessary to ensure the effective prevention of money laundering and terrorism financing. The senior management of the firm must ensure that the policies, procedures, systems and controls are implemented, and that they appropriately and adequately address the requirements of the AML/CFT Law and these rules.

II. **Rules 1.3.3 What is a DNFBP?**

Previous –

What is a *DNFBP*?

(1) A ***designated non-financial business or profession*** (or ***DNFBP***) is any of the following:
- (a) a real estate agent, if the agent acts for clients in relation to the buying or selling of real estate (or both);
- (b) a dealer in precious metals or stones, if the dealer engages in cash transactions with customers with a value (or, for transactions that are or appear to be linked, with a total value) of at least 55,000 Riyals (or its equivalent in any other currency at the relevant time);

New –

1.3.3 What is a *DNFBP*?

(1) A ***designated non-financial business or profession*** (or ***DNFBP***) is any of the following:

(a) a real estate agent, if the agent acts for clients in relation to the buying or selling of real estate (or both);

(b) a dealer in precious metals or stones, if the dealer engages in cash transactions with customers with a value (or, for transactions that are or appear to be linked, with a total value) of at least QR 50,000;

III. **Rules 1.3.8 What is a shell bank?**

Previous –

(2) For this rule, physical presence in a jurisdiction is a presence involving meaningful decision-making and management and not merely the presence of a local agent or low level staff.

New –

(2) For this rule, ***physical presence*** in a jurisdiction is a presence involving effective management that has the authority to make decisions, and not merely the presence of a local agent or low-level staff.

IV. **Part 2.1 - The firm – Rule 2.1.1 - Firms to develop AML/CFT programme**

New –

(5) The firm must make and keep a record of the results of its review and testing under subrule (4) and must give the Regulator a copy of the record by 31 July 2021 and every 2 years thereafter.

V. **Part 2.1 - The firm – Rule 2.1.3 – Matters to be covered by policies etc**

New –

(g) set out the conditions that must be satisfied to permit a customer to use the business relationship even before the customer's identity (or the identity of the beneficial owner of the customer) is verified;
Note For the situations when verification of identity may be delayed, see rules 4.3.5 and 4.5.1 (2).

(h) ensure that there are appropriate systems and measures to enable the firm to implement any targeted financial sanction that may be required under Law No. (27) of 2019 on Combating Terrorism, and for complying with any other requirements of that law; and

VI. **2.1.6 Application of AML/CFT Law requirements, policies etc to branches and associates**

Previous –

(7) If the law of another jurisdiction prevents the application of a provision of this rule to the branch or associate or any of its officers, employees, agents or contractors, the firm must immediately tell the Regulator about the matter.

New –

(7) If the law of another jurisdiction prevents a provision of this rule from applying to the branch or associate or any of its officers, employees, agents or contractors, the firm:

(a) must immediately tell the Regulator about the matter; and

(b) must apply additional measures to manage the money laundering and terrorism financing risks (for example, by requiring the branch or associate to give to the firm additional information and reports).

(8) If the Regulator is not satisfied with the additional measures applied by the firm under subrule (7) (b), the Regulator may, on its own initiative, apply additional supervisory measures by, for example, directing the firm:

(a) in the case of a branch—to suspend the transactions through the branch in the foreign jurisdiction; or

(b) in the case of an associate—to suspend the transactions of the associate insofar as they relate to Qatar.

VII. **Part 2.2 - Senior management - 2.2.2 Particular responsibilities of senior management**

New –

(j) that all reasonable steps have been taken so that a report required to be given to the Regulator for AML or CFT purposes is accurate, complete and given promptly.

VIII. **Part 2.3 MLRO and Deputy MLRO - 2.3.2 Eligibility to be MLRO or Deputy MLRO**

New –

(1) The MLRO and Deputy MLRO for a firm:
(a) must be employed at the management level by the firm, or by a legal person in the same group, whether as part of its governing body, management or staff; and
(b) must have sufficient seniority, knowledge, experience and authority for the role, and in particular:
(i) to act independently; and
(ii) to report directly to the firm's senior management.

IX. **2.3.4 Particular responsibilities of MLRO**

New –

(2) If the Regulator issues guidance, the MLRO must bring it to the attention of the firm's senior management. The firm must make and keep a record of:
(a) whether the senior management took the guidance into account;
(b) any action that the senior management took as a result; and
(c) the reasons for taking or not taking action.

X. **Chapter 3 - The risk-based approach - 3.1.1 Firms must conduct risk assessment and decide risk mitigation**

New –

(1) A firm:
(a) must conduct, at regular and appropriate intervals, an assessment (a business risk assessment) of the money laundering and terrorism financing risks that it faces, including risks identified in the National Risk Assessment and those that may arise from:

Schedule 2 (i) the types of customers that it has (and proposes to have) (***customer risk***);

Schedule 3 (ii) the products and services that it provides (and proposes to provide) (***product risk***);

Schedule 4 (iii) the technologies that it uses (and proposes to use) to provide those products and services (***interface risk***); and

Schedule 5 (iv) the jurisdictions with which its customers are (or may become) associated (***jurisdiction risk***); and

Schedule 6 Examples of 'associated' jurisdictions for a customer

Schedule 7 1 the jurisdiction where the customer lives or is incorporated or otherwise established

Schedule 8 2 each jurisdiction where the customer conducts business or has assets.

Schedule 9 (b) must decide what action is needed to mitigate those risks.

(2) The firm must be able to demonstrate:

Schedule 10 (a) how it determined the risks that it faces;

Schedule 11 (b) how it took into consideration the National Risk Assessment and other sources in determining those risks;

Schedule 12 (c) when and how it conducted the business risk assessment; and

Schedule 13 (d) how the actions it has taken after the assessment have mitigated, or have failed to mitigate, the risks it faces.

Schedule 14 (3) If the firm fails to take into account the National Risk Assessment and other sources or fails to assess any of the risks it faces, it must give the reasons for its failure to do so, if required by the Regulator.

XI. **3.2.5 Measures for PEPs**

New –

The firm must take the measures required by subrule (1) in relation to a family member or close associate of a PEP if, on a risk-sensitive basis, the firm considers that the family member or close associate should be treated as a PEP.

Note: this rule should be interpreted as EDD is required in all cases for family members or close associates of PEPs. The rule will be clarified to reflect the policy intention in the next available round of rulemaking.

XII. **3.2.7 Measures for persons in terrorist list**

New –

(1) A firm must, from the outset of its dealings with an applicant for business and on an ongoing basis during the business relationship, check whether the person is listed:

under a relevant resolution of the UN Security Council; or

in a Terrorist Designation Order published by the National Counter Terrorism Committee of the State.

(2) If the person is listed, the firm:

(a) must not establish, or continue, a relationship with, or carry out a transaction with or for the person;

(b) must make a suspicious transaction report to the FIU; and

(c) must immediately tell the Regulator.

XIII. **3.3.7 Payable-through accounts**

New –

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

XIV. **3.3.9 Bearer negotiable instruments**

Previous –

(1) In this rule:
bearer instrument means—
(a) a bearer share; or
(b) a share warrant to bearer.

(2) A firm must have adequate AML/CFT customer due diligence policies, procedures, systems and controls for risks related to the use of bearer instruments.

(3) Before becoming involved in or associated with a transaction involving the conversion of a bearer instrument to registered form, or the surrender of coupons for a bearer instrument for payment of dividend, bonus or a capital event, a firm must conduct enhanced customer due diligence measures for the holder of the instrument and any beneficial owner.

(4) For subrule (3), the holder and any beneficial owner are taken to be customers of the firm.

New –

(1) In this rule:
bearer negotiable instrument means:
(a) a monetary instrument in bearer form such as a traveller's cheque;
(b) a negotiable instrument, including cheque, promissory note, and money order that is either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery;
(c) an incomplete instrument including a cheque, promissory note and money order signed, but with the payee's name omitted;
(d) a bearer share; or
(e) a share warrant to bearer.

(2) A firm must have adequate AML/CFT customer due diligence policies, procedures, systems and controls for risks related to the use of bearer negotiable instruments.

(3) Before becoming involved in or associated with a transaction involving the conversion of a bearer negotiable instrument, or the surrender of coupons for a

bearer negotiable instrument for payment of dividend, bonus or a capital event, a firm must conduct enhanced CDD for the holder of the instrument and any beneficial owner.

(4) For subrule (3), the holder and any beneficial owner are taken to be customers of the firm.

XV. **3.3.10 Wire transfers**

New –

(1) This rule applies to a transaction conducted by a financial institution (the ordering financial institution) by electronic means on behalf of a person (the originator) with a view to making an amount of money available to a person (the recipient) at another financial institution (the beneficiary financial institution).

(2) This rule applies to the transaction whether or not:

(a) the originator and recipient are the same person;

(b) the transaction is conducted through intermediary financial institutions; or

(c) the ordering financial institution, the beneficiary financial institution or any intermediary financial institution is outside Qatar.

(3) However, this rule does not apply to a transaction conducted using a credit or debit card if:

(a) the card number accompanies all transfers flowing from the transaction; and

Examples of transfers that may flow from the transaction

1 withdrawals from a bank account through an ATM

2 cash advances from a credit card

3 payments for goods and services

(b) the card is not used as a payment system to effect a money transfer.

(4) Also, this rule does not apply:

(a) to transfers from 1 financial institution to another; or

(b) if the originator and recipient are both financial institutions acting on their own behalf.

(5) If the ordering financial institution is in Qatar, it:

(a) must obtain and keep full originator information; and

(b) must conduct CDD for the originator;

unless the beneficiary financial institution and all intermediary financial institutions (if any) are in Qatar and the transaction involves the transfer of less than QR 3,500.

Note Full originator information is defined in the Glossary.

(6) To remove any doubt, the ordering financial institution needs only to comply with subrule (5) once for the originator.

(7) If the ordering financial institution is in Qatar and the beneficiary financial institution or any intermediary financial institution is outside Qatar, the ordering financial institution must include full originator information and full recipient information in a message or payment form accompanying the transfer.

Note Full recipient information is defined in the Glossary.

(8) However, if several separate transfers from the same originator are bundled in a batch file for transmission to several recipients in a foreign jurisdiction, the ordering financial institution needs only to include the originator's account number or unique reference number in relation to each individual transfer if the batch file (in which the individual transfers are batched) contains full originator information, and full recipient information for each recipient, that is fully traceable in the foreign jurisdiction.

(9) If the ordering financial institution, the beneficiary financial institution and all intermediary financial institutions (if any) are in Qatar, the ordering financial institution must include full originator information and full recipient information in a message or payment form accompanying the transfer unless:

(a) the transaction involves the transfer of less than QR 3,500;

or

(b) both of the following conditions are satisfied:

(i) full originator information and full recipient information can be made available to the beneficiary financial institution, the Regulator, the FIU and law enforcement authorities within 3 business days after the day the information is requested;

(ii) law enforcement authorities can compel immediate production of the information.

(10) Each intermediary financial institution (if any) must ensure that all information relating to the originator and recipient that the financial institution receives in a message or payment form accompanying the transfer is transmitted to the next financial institution.

(11) If the beneficiary financial institution is in Qatar and is aware that full originator information or full recipient information has not been provided in a message or payment form accompanying the transfer (and is not fully traceable using a batch file as mentioned in subrule (8)), it must:

(a) either:

(i) reject the transfer; or

(ii) obtain the missing or incomplete information from the ordering financial institution; and

(b) using a risk-sensitive approach, decide whether a suspicious transaction report should be made to the FIU.

(12) If the ordering financial institution has regularly failed to provide the required information about the originators or recipients of transactions and the beneficiary financial institution is in Qatar, the beneficiary financial institution:

(a) must take appropriate steps to ensure that the ordering financial institution does not contravene this rule; and

(b) must report the matter to the FIU.

Examples of steps

1 issuing warnings and setting deadlines for the provision of information

2 rejecting future transfers from the ordering financial institution

3 restricting or terminating any business relationship with the ordering financial institution

(13) Despite anything in these rules, no money or value may be transferred by electronic means to a person listed:

(a) under a relevant resolution of the UN Security Council; or

(b) in a Terrorist Designation Order published by the National Counter Terrorism Committee of the State.

3.3.11 Additional obligations of firms involved in wire transfers

(1) A firm that acts as an intermediary financial institution in a cross-border wire transfer and a firm (the beneficiary financial institution) that makes money available to the recipient after the cross-border wire transfer must take reasonable measures, on a risk-sensitive basis, to identify transfers to this jurisdiction that lack full originator information or full recipient information. The measures may include following-up (whether during, or after, the transfer) on information that is lacking about the originator or recipient.

(2) A firm that acts as intermediary financial institution or beneficiary financial institution must develop, establish and maintain policies, procedures, systems and controls to determine:

(a) when to execute, reject or suspend a wire transfer that lacks the full originator information or full recipient information; and

(b) when to take appropriate follow-up action.

(3) A firm that acts as intermediary financial institution in a cross-border wire transfer must ensure that all originator and recipient information accompanying the transfer is retained with it.

(4) A firm that acts as ordering financial institution, intermediary financial institution or beneficiary financial institution must keep full originator information and full recipient information for at least 10 years after:

(a) if the firm acted as ordering financial institution—the day the originator asked the firm to make the wire transfer;

(b) if the firm acted as intermediary financial institution—the day the firm transmitted the information to another intermediary or to the beneficiary financial institution; or

(c) if the firm acted as beneficiary financial institution—the day the money received via wire transfer is made available to the recipient.

(5) If a wire transfer between 2 financial institutions in Qatar (domestic wire transfer) is necessary to effect a cross-border wire transfer and, because of technical limitations, the full originator

information and full recipient information cannot remain with the domestic wire transfer, the intermediary financial institution to which the domestic wire transfer is made must, if the intermediary financial institution is a firm, make and keep a record of the information received by it from the ordering financial institution or other intermediary financial institution in relation to the transaction. The record must be kept for 10 years after the day it is made.

(6) If a cross-border wire transfer is effected by the same firm as both ordering and beneficiary financial institutions, or if a firm controls both the originator and recipient of the wire transfer, the firm must take into account the information obtained from both sides of the transfer in considering whether to make a suspicious transaction report. If the firm suspects that the transfer may involve money laundering or terrorism financing, it must:

(a) make a report in each jurisdiction affected by the transfer; and

(b) make available, to the FIU (or its equivalent) in the jurisdiction, information relevant to the transfer.

(7) For wire transfers of more than QR 3,500, the beneficiary financial institution must verify the identity of the recipient before making money available, except if the recipient's identity has previously been verified.

XVI. **Division 3.4.B Reliance on others generally - 3.4.8 Reliance on certain third parties generally**

New –

(3) In determining whether to rely on a third party for purposes of this rule, the firm must have regard to any relevant findings published by international organisations, governments and other bodies about the jurisdiction where the third party is located.

XVII. **3.4.10 Group introductions**

New –

(2) The local firm need not satisfy itself that all of the conditions in subrule (1) (b) have been met if the Regulator (or the equivalent regulatory or governmental authority, body or agency in another jurisdiction where the relevant financial institution is established) has determined that:

(a) the group's AML/CFT programme, CDD and record-keeping requirements comply with AML/CFT Law and these rules;

(b) the group's implementation of the programme and compliance with the requirements are subject to effective consolidated supervision by the Regulator or its equivalent; and

(c) the group's AML/CFT policies, procedures, systems and controls adequately mitigate risks related to operations in high risk jurisdictions.

XVIII. **Part 4.2 Know your customer—key terms - 4.2.1 What is *customer due diligence*?**

New –

(1) Customer due diligence (or CDD), in relation to a customer of a firm, is all of the following measures:

(a) identifying the customer;

(b) verifying the customer's identity using reliable, independent source documents, data or information;

(c) establishing whether the customer is acting on behalf of another person (in particular whether the customer is acting as a trustee);

Schedule 15 (4) If the customer is a legal person or legal arrangement, and a person purporting to act on behalf of the customer is not a beneficial owner of the customer, CDD also includes:

Schedule 16 (a) identifying the beneficial owner; and

Schedule 17 (b) verifying the beneficial owner's identity using reliable, independent source documents, data or information.

Schedule 18

Schedule 19 (5) For subrule (3) (e) (ii), examples of the measures required include:

Schedule 20 (a) if the customer is a company—identifying the individuals with a controlling interest and the individuals who comprise the mind and management of the customer; and

Schedule 21 *Note* See rule 4.6.8 (Customer identification documentation—corporations).

Schedule 22 (b) if the customer is a legal arrangement—identifying the parties to the arrangement, including the person exercising effective control over the arrangement.

Schedule 23 *Note* See rule 4.3.9 (Extent of CDD—legal persons and arrangements) and rule 4.6.11 (Customer identification documentation—legal arrangements).

XIX. **4.2.4 What is a business relationship?**

Previous –

A business relationship, in relation to a firm, is a business, professional or commercial relationship between the firm and a customer, other than a relationship that is reasonably expected by the firm, when contact is established, to be merely transitory.

New –

A business relationship means a regular relationship between a customer and a firm in connection with a service that the customer receives from the firm.

Note A relationship that, when contact is established, is reasonably expected by a firm to be merely transitory does not constitute a business relationship.

XX. **4.3.2 When CDD required—basic requirement**

Previous –

(1) A firm must conduct customer due diligence measures for a customer when—

(a) it establishes a business relationship with the customer; or

(b) it conducts a one-off transaction for the customer with a value (or, for transactions that are or appear (whether at the time or later) to be linked, with a total value) of at least the threshold amount; or

New –

(1) A firm must conduct CDD for a customer when:

(a) it establishes a business relationship with the customer;

(b) it conducts a one-off transaction for the customer with a value (or, for transactions that are or appear (whether at the time or later) to be linked, with a total value) of at least QR 50,000;

Note A firm must have systems and controls to identify one-off transactions that are linked to the same person (see rule 4.3.15 (1)).

XXI. **4.3.3 Firm unable to complete CDD for customer**

Previous –

(1) This rule applies if a firm cannot complete customer due diligence measures for a customer.

Examples

1 the firm is unable to verify the customer's identity using reliable, independent source, data or information

2 the customer exercises cancellation or cooling-off rights

(2) The firm must—

(a) immediately terminate any relationship with the customer; and

(b) consider whether it should make a suspicious transaction report to the FIU.

Note See r 5.1.7 (Obligation of firm to report to FIU etc).

New –

(1) This rule applies if a firm cannot complete CDD for a customer.

Examples

1 the firm is unable to verify the customer's identity using reliable, independent source, data or information

2 the customer exercises cancellation or cooling-off rights

(2) The firm:

(a) must immediately terminate any relationship with the customer;

(b) must not establish a relationship with, or carry out a transaction with or for, the customer; and

(c) must consider whether it should make a suspicious transaction report to the FIU.

XXII. **4.3.5 Timing of CDD—establishment of business relationship**

New –

(2) However, the CDD may be conducted during the establishment of the relationship if:

(a) this is necessary in order not to interrupt the normal conduct of business; and

Examples of where it may be necessary in order not to interrupt the normal conduct of business

1 non-face-to-face business

2 securities transactions

(b) there is little risk of money laundering or terrorism financing and these risks are effectively managed;

Examples of measures to effectively manage risks

1 limiting the number, types and amount of transactions that may be conducted during the establishment of the relationship

2 monitoring large or complex transactions being carried out outside the expected norms for the relationship

(c) the CDD is completed as soon as practicable after contact is first established with the customer; and

(d) the CDD is conducted in accordance with the policies, procedures, systems and controls on the use of the business relationship even before the customer's identity is verified.

(5) If the firm establishes a business relationship with the customer under subrule (2), (3) or (4) but cannot complete CDD for the customer, the firm:

(a) must immediately terminate any relationship with the customer;

(b) must not carry out a transaction with or for the customer; and

(c) must consider whether it should make a suspicious transaction report to the FIU.

Note Under rule 2.1.3 (2) (g), a firm must have policies, procedures, systems and controls that set out the conditions that must be satisfied to permit a customer to use the business relationship even before the customer's identity (or the identity of the beneficial owner of the customer) is verified.

XXIII. **4.3.6 Timing of CDD—one-off transactions**

New –

(2) If the firm cannot complete CDD for the customer, the firm:

(a) must immediately terminate any relationship with the customer;

(b) must not carry out the transaction with or for the customer; and

(c) must consider whether it should make a suspicious transaction report to the FIU.

XXIV. **4.3.9 Extent of CDD—legal persons and arrangements**

Previous –

(3) However, if the customer due diligence measures are required to be conducted for a trust and the beneficiaries and their contributions have already been decided, the firm must identify each beneficiary who is to receive at least 25% of the funds of the trust (by value).

Note See also r 4.6.11 (Customer identification documentation—trusts).

New –

(3) However, if the CDD is required to be conducted for a legal arrangement and the beneficiaries and their contributions have already been decided, the firm must identify each beneficiary

who is to receive at least 20% of the funds of the arrangement (by value).

Note See also rule 4.6.11 (Customer identification documentation—legal arrangements).

XXV. **4.3.10 CDD for beneficiaries of life insurance policies—general**

New –

(3) In deciding whether enhanced CDD is applicable, a financial institution must consider the beneficiary of a life insurance policy as a risk factor. If the financial institution decides that a beneficiary who is a legal person or a legal arrangement presents a higher risk, the enhanced CDD should include reasonable measures to identify, and verify the identity of, the beneficiary's beneficial owner at the time of payout.

(4) (4)If a financial institution is unable to comply with this rule, it must consider making a suspicious transaction report to the FIU.

XXVI. **4.3.11 CDD for PEPs as beneficiaries of life insurance policies**

New –

Schedule 24 (1) Before making a payout from a life insurance policy, a financial institution must take reasonable measures to determine whether the beneficiary, or the beneficial owner of the beneficiary, of the policy is a PEP.

Schedule 25 (2) If the beneficiary or its beneficial owner is a PEP and the PEP presents a higher risk, the firm:

Schedule 26 (a) must inform its senior management;

Schedule 27 (b) must conduct enhanced CDD of its business relationship with the policyholder; and

Schedule 28 (c) must make a suspicious transaction report to the FIU.

XXVII. **CDD for purchaser and vendor of real estate**

New –

Schedule 29 A DNFBP acting as real estate agent in relation to a transaction for the sale of real property must conduct CDD on both the buyer and seller of the property (even if the DNFBP acts for only 1 of the parties to the transaction).

Schedule 30

XXVIII. **Part 4.4 Enhanced CDD and ongoing monitoring**

New –

4.4.1 Enhanced CDD and ongoing monitoring—general

A firm must, on a risk-sensitive basis, conduct enhanced CDD and enhanced ongoing monitoring:

(a) in cases where it is required to do so under the AML/CFT Law or these rules;

(b) if required by the Regulator or the NAMLC;

(c) in cases where FATF calls upon its members to require enhanced CDD and enhanced ongoing monitoring; and

(d) in any other case that by its nature can present a higher risk of money laundering or terrorism financing.

XXIX. **4.4.2 Measures required for enhanced CDD or ongoing monitoring**

New –

Chapter 1 A firm that is required to conduct enhanced CDD or enhanced ongoing monitoring must include the following measures, as appropriate to either or both requirements:

Chapter 2 (a) obtain additional information about the customer (for example, profession, volume of assets and information available through public databases and open sources);

Chapter 3 (b) update customer identification and beneficial owner identification;

Chapter 4 (c) obtain additional information on the purpose and intended nature of the business relationship;

Chapter 5 (d) obtain additional information on the sources of the customer's wealth and funds;

Chapter 6 (e) obtain information on the reasons for the expected transactions or the transactions that have been carried out;

Chapter 7 (f) obtain senior management approval before establishing or continuing a business relationship;

Chapter 8 (g) implement additional and continuous controls by identifying transactions and patterns of transactions that need additional scrutiny and review;

Chapter 9 (h) make the first of any required payments to the customer through an account in a bank that is regulated and supervised (at least for AML and CFT purposes) by the Regulator or by an equivalent regulatory or governmental authority, body or agency in another jurisdiction.

XXX. **4.4.3 Measures in addition to enhanced CDD and ongoing monitoring**

New –

Chapter 10 In addition to the enhanced CDD and enhanced ongoing monitoring in this Part, a firm must conduct, on a risk-sensitive basis:

(a) countermeasures proportionate to the risks specified in circulars published by the NAMLC based on relevant findings of international organisations, governments and other bodies; and

(b) other measures determined by the NAMLC on its own initiative.

Chapter 11

XXXI. **Simplified CDD and ongoing monitoring - 4.5.1 Simplified CDD—general**

New –

Except if there is a suspicion of money laundering or terrorism financing, a firm may conduct, for a customer, simplified CDD under rules 4.5.2 to 4.5.4 when:

(a) it establishes a business relationship with the customer; or

(b) it conducts a one-off transaction for the customer to which rule 4.3.2 (1) (b) (When CDD required—basic requirement) applies.

XXXII. **4.5.2 Customer with low level of risk**

New –

A firm may conduct simplified CDD for a customer who presents a low level of risk. The CDD must be commensurate to the level of risk and may include:

(a) despite rule 4.3.5, verifying the identity of the customer or beneficial owner after (rather than before) the business relationship has been established;

(b) despite rule 4.3.6, verifying the identity of the customer or beneficial owner after (rather than before) a one-off transaction with a value of at least QR 50,000;

(c) reducing the intensity, extent and frequency of updates of customer identification; and

(d) not collecting information, or not carrying out measures, to determine the purpose and intended nature of the business relationship, and instead inferring that purpose and nature from the transactions carried out under that relationship.

XXXIII. **4.5.5 Simplified ongoing monitoring**

New –

This Part applies to ongoing monitoring in relation to a customer that presents a low level of risk. The ongoing measures must be commensurate to the level of risk and may include the reduction, based on a reasonable threshold determined by the firm, of the intensity, extent and frequency of:

(a) the firm's scrutiny of the customer's transactions; and

(b) the firm's review of its records of the customer.

XXXIV. **Customer identification documentation - Division 4.6.C Customer identification documentation—particular applicants for business - .6.8 Customer identification documentation—corporations**

New –

(6) If the corporation, or the corporation's parent entity, is listed in a stock exchange that has disclosure requirements that enable the customer's or owner's identity to be verified in a fully transparent way, the firm:

(a) need not identify, nor verify the identity of, the shareholders of the corporation or the shareholders of the parent entity; and

(b) may instead satisfy the customer identification requirements by obtaining information from a public register, the corporation or parent entity itself, or other reliable sources.

XXXV. 4.6.11 Customer identification documentation—legal arrangements

New –

(1)This rule applies if an applicant for business for a firm is a legal arrangement.

(2) In conducting a risk assessment for the legal arrangement, the firm must take into account the different money laundering and terrorism financing risks that are posed by arrangements of different sizes and

areas of activity. This subrule does not limit the matters the firm may take into account.

Examples

Some legal arrangements have a limited purpose (for example, inheritance tax planning) or have a limited range of activities. Others have more extensive activities and connections including financial links with other jurisdictions.

(3) The firm must, as a minimum, obtain the following information about the legal arrangement:

(a) the arrangement's full name;

(b) the nature and purpose of the arrangement;

Examples of the nature of arrangements

discretionary, testamentary, bare

(c) the jurisdiction where the arrangement was established;

(d) the identities of the parties to the arrangement;

Examples of parties to a trust

settlor, trustee, protector and beneficiary

(e) the beneficial owner of the arrangement.

Note Under rule 1.3.5 (1) (c) and 1.3.5 (4), the ***beneficial owner*** of a legal arrangement is the individual who ultimately owns, or exercises effective control over, the arrangement and includes:

(a) if the beneficiaries and their distributions have already been decided—an individual who is to receive at least 20% of the funds of the arrangement; and

(b) if the beneficiaries or their distributions have not already been decided—the class of individuals in whose main interest the arrangement is established or operated as beneficial owner; and

(c) an individual who, directly or indirectly, exercises control over at least 20% (by value) of the property of the arrangement.

(4) The firm must verify the identity of an applicant that is a legal arrangement using reliable, independent source documents, data or information that show:

(a) the name, nature and proof of existence of the arrangement; and

(b) the terms of the arrangement.

(5) The firm must verify that any person purporting to act on behalf of the legal arrangement is so authorised, and must identify and verify the identity of that person.

(6) The firm:

(a) must understand, and if necessary obtain information on, the purpose and intended nature of the business relationship; and

(b) must understand the nature of the business of the legal arrangement and its ownership and control structure.

XXXVI. **4.6.14 Other requirements for customer identification of legal persons**

New –

(1)In addition to the customer identification documentation required for particular applicants under this Division, a firm must verify the identity of an applicant that is a legal person using reliable, independent source documents, data or information that show:

(a) the name, legal form and proof of existence of the legal person;

(b) the mandates, declarations, resolutions and other sources of power that regulate and bind the legal person;

(c) the names of the persons holding senior management positions in the legal person; and

(d) the address of the registered office of the legal person and, if different, its principal place of business.

(2)The firm must verify that any person purporting to act on behalf of the legal person is so authorised, and must identify and verify the identity of that person.

(3)The firm must:

(a) understand, and if necessary obtain information on, the purpose and intended nature of the business relationship; and

(b) understand the nature of the business of the legal person and its ownership and control structure.

(4)For subrule (3) (b), the firm must identify, and verify the identity of:

(a) the individual who is the beneficial owner of the legal person; or

(b) if no individual can be identified as the beneficial owner of the legal person (or if there is doubt that an individual is the beneficial owner)—the legal person's most senior manager.

Note Under rule 1.3.5 (1) (c) and 1.3.5 (3), the ***beneficial owner*** of a legal person is the individual who ultimately owns, or

exercises effective control over, the person and includes, for a corporation:

(a) an individual who, directly or indirectly, owns or controls at least 20% of the shares or voting rights of the corporation; and

(b) an individual who, directly or indirectly, otherwise exercises control over the corporation's management.

XXXVII. **Division 5.1.A Reporting requirements—general - 5.1.7 Obligation of firm to report to FIU etc**

New –

Schedule 31 (3) The report must be made on the firm's behalf by:

Schedule 32 (a) the MLRO; or

Schedule 33 (b) if the report cannot be made by the MLRO (or Deputy MLRO) for any reason—by a person who is employed (as described in rule 2.3.2 (1) (a)) at the management level by the firm, or by a legal person in the same group, and who has sufficient seniority, knowledge, experience and authority to investigate and assess internal suspicious transaction reports.

Schedule 34

Schedule 35 (5) The report must be made in the form (if any) approved by the FIU, and in accordance with the unit's instructions. The report must include a statement about:

Schedule 36 (a) the facts or circumstances on which the firm's knowledge or suspicion is based or the grounds for the firm's knowledge or suspicion; and

Schedule 37 (b) if the firm knows or suspects that the funds belong to a third person—the facts or circumstances on which that knowledge or suspicion is based or the grounds for the firm's knowledge or suspicion.

Schedule 38

XXXVIII. **5.1.9 Firm may restrict or terminate business relationship**

New –

If the firm restricts or terminates a business relationship with a customer, it must immediately tell the Regulator about the restriction or termination.

XXXIX. **Part 5.2 Tipping-off - 5.2.2 Firm must ensure no tipping-off occurs**

New –

Schedule 39 (1) A firm must ensure that:

Schedule 40 (a) its officers and employees are aware of, and sensitive to:

Schedule 41 (i) the issues surrounding tipping-off; and

Schedule 42 (ii) the consequences of tipping-off; and

Schedule 43 (b) it has policies, procedures, systems and controls to prevent tipping-off within the firm or its group.

Schedule 44

XL. **5.2.4 When advice not considered to be tipping-off**

New –

(1) This rule applies to lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals.

(2) The act of a lawyer, notary, other legal professional or accountant in disclosing relevant information in the course of advising a person against engaging in an illegal act does not constitute tipping-off.

Section 3: Record Keeping

Chapter 7 -Providing documentary evidence of compliance - 7.1.2 - How long records must be kept

The time required for record retention has increased for authorised firms and designated non-financial businesses and professions from a minimum of six years to at least 10 years.

Amendments to AMLG (in addition to amendments set out in AML/CFTR section of this note).

I. **Part 2.1 - The firm 2.1.1-Firms to develop AML/CFT programme**

New –

Schedule 45 (3) However, the programme must, as a minimum, include:

Schedule 46 (a) developing, establishing and maintaining internal policies, procedures, systems and controls to identify and prevent money laundering and terrorism financing;

Schedule 47 (b) adequate screening procedures to ensure high standards when appointing or employing officers or employees;

Chapter 12 *Note* See also Part 6.1 (Screening procedures).

Schedule 48 (c) an appropriate ongoing training programme for its officers and employees;

Chapter 13 *Note* See also Part 6.2 (AML/CFT training programme).

Schedule 49 (d) an independent review and testing of the firm's compliance with its AML/CFT policies, procedures, systems and controls in accordance with subrule (4);

Schedule 50

Schedule 51 (4) The review and testing of the firm's compliance with its AML/CFT policies, procedures, systems and controls must be adequately resourced and must be conducted at least once every 2 years. The person making the review must be professionally competent, qualified and skilled, and must be independent of:

Schedule 52 (a) the function being reviewed; and

Schedule 53 (b) the division, department, unit or other part of the firm where that function is performed.

Chapter 14 *Note* The review and testing may be conducted by the firm's internal auditor, external auditor, risk specialist, consultant or an MLRO from another branch of the firm. Testing would include, for example, sample testing the firm's AML/CFT programme, screening of employees, record making and retention and ongoing monitoring for customers.

Schedule 54 (5) The firm must make and keep a record of the results of its review and testing under subrule (4) and must give the Regulator a copy of the record by 31 July 2021 and every 2 years thereafter.

Schedule 55

Schedule 56

II. **2.2.2 Particular responsibilities of senior management**

New –

(1) The senior management of a firm must ensure:

Schedule 57 (d) that independent review and testing of the firm's compliance with its AML/CFT policies, procedures, systems and controls are conducted in accordance with rule 2.1.1 (4);

Chapter 15