هيئة تنظيم مركز قطر للمال
QATAR FINANCIAL CENTRE
REGULATORY AUTHORITY

Guidance on Customer Due Diligence

TABLE OF CONTENTS

Version control:

Guidance on Customer Due Diligence
V2.0
March 2020

GLOSSARY OF TERMS

AML/CFT	Anti-Money Laundering/Combating the Financing of Terrorism
AML/CFT Law	State of Qatar Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing
Competent Authority	An AML/CFT Regulator in the State of Qatar or the Qatar Financial Centre
CDD	Customer Due Diligence
DNFBP	Designated Non-Financial Businesses and Professions
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIRM	A Financial Institution or a DNFBP operating in the State of Qatar or the Qatar Financial Centre
KYC	Know Your Customer
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
NAMLC	Qatar National Anti-Money Laundering and Terrorism Financing Committee
NCTC	Qatar National Counter Terrorism Committee
NRA	Qatar National AML/CFT Risk Assessment
PEP	Politically Exposed Person
PPSC	Policies, Procedures, Systems and Controls
QCB	Qatar Central Bank
QFC	Qatar Financial Centre
QFCRA	Qatar Financial Centre Regulatory Authority
QFIU	Qatar Financial Information Unit
QFMA	Qatar Financial Markets Authority
SDD	Simplified Due Diligence
STR	Suspicious Transaction Report
TF	Terrorism Financing

1. PURPOSE

The purpose of this document is to provide practical guidance to Firms on Customer Due Diligence. It is provided to assist Firms with day-to-day compliance challenges and provide examples of international best practice.

The guidance cannot address every possible scenario and is not legal advice. It does not replace the AML/CFT Law or other relevant AML/CFT legislation applicable in the State of Qatar or the Qatar Financial Centre. Firms remain responsible for compliance with relevant legislation.

2. WHAT IS CUSTOMER DUE DILIGENCE (CDD)

To effectively prevent ML and TF, a Firm must know who they are dealing with, the nature of their business, where their money comes from, and where their money is going.

CDD is the process a Firm uses to identify their customer, understand the customer's business and the source and destination of their funds. This includes:

- identifying the customer and verifying the customer's identity with documents, data or information from reliable and independent sources;
- identifying the customer's beneficial owners and taking reasonable steps to verify their identity, so that the Firm is satisfied that it knows who the beneficial owner is;
- identifying persons acting on behalf of a customer, taking reasonable steps to verify their identity, and verifying that they are authorised to act on behalf of the customer;
- screening customers and other relevant entities and persons to ensure the Firm does not contravene NCTC sanctions, United Nations sanctions, or other sanctions relevant to the Firm's business;
- obtaining appropriate information to understand the purpose and intended nature of the business relationship with the customer;
- taking appropriate steps to understand the flow of funds resulting from the business relationship, including the source of funds and the ultimate destination of the funds;
- conducting ongoing monitoring of the business relationship, including transaction monitoring;
- ensuring that business activities are consistent with the Firm's knowledge of the customer; and
- ensuring that information collected by the Firm about the customer remains up to date.

3. WHEN TO CONDUCT CDD

CDD must be done whenever it is required by the particular circumstances of a Firm's relationship with the customer. This includes:

- when the Firm first establishes a business relationship with the customer;
- when conducting a transaction for an occasional customer where the value exceeds QAR 55,000 or its equivalent in foreign currency;
- when conducting a series of transactions for an occasional customer which occur close in time or appear to be linked, and the value in aggregate exceeds QAR 55,000 or its equivalent in foreign currency;
- when conducting a wire transfer originating in Qatar that exceeds a threshold of QAR 3,500;
- when a customer's circumstances change;
- when there is a significant change in the customer's business;
- when the Firm has doubts about the existing information it holds on a customer;
- when the Firm suspects Money Laundering (ML) or Terrorism Financing (TF).

4. DELAY OF CDD

CDD should be completed at the commencement of the Firm's relationship with the customer, and no work or transactions should be undertaken until CDD is complete. In very limited circumstances, CDD can be completed during the course of a business relationship. Those limited circumstances are:

- it is necessary in order not to interrupt the normal conduct of business;
- there is little risk of ML or TF and these risks are effectively managed; and
- CDD is completed as soon as possible after first contact with the customer.

There should be strict controls over any deferral of CDD, including regular tracking and reporting to senior management to ensure that CDD is completed. It is important to restrict account activity during this period – outward/debit payments should not be permitted until CDD requirements are satisfied. If it is not possible to complete CDD in a timely manner, the Firm must terminate the business relationship with the customer. The Firm should also consider whether it is appropriate to file a Suspicious Transaction Report (STR) with the Qatar Financial Information Unit (QFIU). The Firm should ensure that it does not tip off the customer. Tipping off is defined in paragraph 22 below.

5. KEEPING CDD UP TO DATE

A Firm should review the information it holds on a customer at regular intervals and ensure that this information is up to date. The frequency of review will be determined by the Firm's risk rating of the customer.

If there is a change in the customer's circumstances, such as a change in business activity or ownership, the Firm should also review its risk assessment of the customer and whether further CDD is required.

Generally, a Firm can rely on the CDD it has already undertaken unless it has doubts about the accuracy and reliability of that information, or it becomes out of date. However CDD should be reviewed where there are doubts, for example if there is a suspicion of ML or TF, where there is a material change in the customer's account or business activity which is inconsistent with the customer's business profile.

6. GENERAL CONSIDERATIONS REGARDING DOCUMENTS

Information about a customer must be verified using documents, data and information obtained from reliable and independent sources. This information should be current at the time it is obtained.

Documents should be clear and legible, including the photograph on customer identification documents.

The best documents to rely upon are those that are most difficult to counterfeit or obtain illicitly. This includes government issued identity cards, passports, reports from independent business and company registries, audited annual reports and other reliable sources of information.

When copy documents are relied on, they should be verified by an authorised staff member of the Firm sighting the original. Details of the verification should be recorded. If an original cannot be produced, the Firm may consider accepting a copy that is certified as a true copy by a notary public, lawyer or some other suitably qualified professional.

If a document is in a foreign language, the Firm should take appropriate steps, independent of the customer, to ensure that it understands the nature of the document and its content. This may be done by a staff member of the Firm conversant in the language providing a written summary of the key aspects of the document. Alternatively, a suitably qualified translator may be engaged by the Firm.

7. RECORD KEEPING

All Firms operating in the State of Qatar and in the QFC must retain relevant CDD records for at least ten years after the end of the business relationship. Records may be electronic and/or hard copy.

All documents and records obtained through CDD measures must be kept. This includes:

- Copies or records of official identification documents such as passports, identity cards, driving licences, or similar documents;
- Evidence of sanctions screening (at onboarding and on an ongoing basis);
- Account files and business correspondence;
- Analysis conducted by the Firm, such as inquiries to establish the background and purpose of complex, unusual large transactions.

The CDD records that must be kept include all necessary records on transactions, both domestic and international, to enable a Firm to comply swiftly with information requests from Competent Authorities. These records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for the prosecution of criminal activity.

PART 2 – PARTICULAR MEASURES

8. IDENTITIFYING AND VERIFYING THE IDENTITY OF A NATURAL PERSON

A Firm should identify a customer who is a natural person by obtaining their full name, date of birth and nationality based on a valid passport or a national identity card that bears a clear photograph of the customer. If a customer holds dual nationality, Firms should consider whether this has an impact on the customer's risk profile (for further information see the guidance paper on "The Risk Based Approach").

Where possible the customer's residential address should be verified. While obtaining documents showing a residential address may be difficult in Qatar, some documents which may available include:

- a residential tenancy lease;
- a Kahraama statement; or
- a letter from the customer's employer.

The Firm should obtain similar verification documents for a non-resident customer. The type of documents obtained will depend upon what sort of verification documents are available in the jurisdiction where the customer is located, e.g. utility bills.

If it is not possible to verify a customer's residential address, the Firm should consider whether verifying other available information, such as a postal or business address is adequate given the risk profile of the customer.

9. IDENTIFYING AND VERIFYING THE IDENTITY OF A LEGAL PERSON OR LEGAL ARRANGEMENT

A Firm should identify a customer who is a legal person or legal arrangement including understanding the nature of its business, its ownership and its control structure. The type of information needed to do this includes:

- Name, legal form and proof of existence, verified by a certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust or other documentation from a reliable independent source proving the name, form and current existence of the customer;
- The powers that regulate and bind the legal person or arrangement (e.g. the memorandum and articles of association of a company), as well as the names of the relevant persons having a senior management position in the legal person or arrangement (e.g. senior managing directors of a company, trustees of a trust); and
- The registered office address and the principal place of business (if different).

Appendix 1 contains examples by customer type of particular CDD information a Firm may consider obtaining.

A Firm should also identify and take reasonable steps to verify the identity of the beneficial owners who own or control 20% or more of a customer. In higher risk scenarios, a Firm may wish to use a lower threshold, in recognition of the increased risk

The type of verified information needed to identify beneficial owners of a legal person includes:

- The identity of the natural persons exercising control of the legal person who ultimately have a controlling ownership interest in a legal person; or
- The identity of the natural persons exercising control of the legal person through other means, if a natural person exercising control through an ownership interest cannot be identified; or
- The identity of the relevant natural person who hold the position of senior managing official; if a natural person exercising control through ownership or other means cannot be identified.

The type of verified information needed to identify beneficial owners of a legal arrangement includes:

- Trusts – the identity of the settlor, the trustees, the protector (if any), the beneficiaries or class of beneficiaries and any other natural person exercising ultimate effective control over the trust (including through a chain of control or ownership;
- Other types of legal arrangements – the identity of persons in equivalent or similar positions.

Beneficial ownership, including beneficiaries of life insurance policies, is discussed in detail in a separate guidance paper: "Beneficial Ownership of Legal Persons and Legal Arrangements".

10. USE RELIABLE SOURCES OF DOCUMENTATION TO VERIFY IDENTIFY

Firms should only accept documents from reliable official sources to verify identity, or the nature and existence of the legal person or legal arrangement.

The original identity document should be sighted by a staff member of the Firm and a copy should be retained by the Firm. If it is not possible to keep a copy of the identify document, the Firm should record its unique identification number and any relevant observations about its condition, e.g. if it was worn or ripped etc. The reason why a copy could not be obtained should be recorded.

Copies of original identity documents must be legible and certified as "original seen" by a staff member. Uncertified copies should not be accepted directly from a

customer unless a staff member has compared it to the original document and can vouch for the veracity of the copy. Copies of copies should never be accepted.

A risk-based approach may be taken to verification of identity of natural persons in specific limited circumstances. It may be impractical or impossible to obtain identification documentation of very high profile public figures, such as the most senior members of royal families. Extensive public information is normally available on such persons from reliable and verifiable sources, and therefore Firms may build and keep on the customer file an identity profile for the prominent person as an alternative to requesting physical identification documents. However, this practice should only be used:

- as an exception, not as a general approach to verification of identity; and
- where reasonable and justifiable; and
- where there are no other risk factors which reasonably suggest normal verification processes should apply, either at onboarding or at any stage in the business relationship; and
- where there are approved written procedures to guide staff; and
- where senior management approves each case where the exception is used; and
- where there is Compliance oversight to ensure that the exception is not being misused.

11. POLITICALLY EXPOSED PERSONS (PEP)

A PEP is an individual who is, or has been, entrusted with prominent public functions by the State of Qatar; by a foreign State; or by an international organisation. Firms should have appropriate risk management systems to determine if a customer, a person in control of the customer, or the beneficial owner of a customer, is a PEP.

A Firm should exercise sound judgment in identifying PEPs and consider multiple sources of information, such as:

- information from the customer;
- local staff knowledge;
- internet searches; and
- commercial databases.

Firms should be aware of the limitations of commercial databases. The presence or absence of a name in a database should not prevent further enquiry, as database providers may use PEP definitions that are different to those used by a Firm.

The Firm's reasons for deciding whether or not a person is a PEP should be clearly recorded.

Where PEPs are identified, Enhanced Due Diligence (EDD) should be undertaken, including:

- Obtaining senior management approval to establish the relationship (or annual review and approval to continue or end the relationship for existing customers);
- Taking reasonable measures to establish the source of wealth and source of funds; and
- Conducting enhanced ongoing monitoring of the business relationship.

The additional measures for PEPs should also be applied to family members or close associates of PEPs. When determining whether a person is a close associate of a PEP, the Firm may consider factors such as the level of influence the PEP has on the person or the extent of their exposure to the PEP (e.g. do they have common business ownership). The Firm may rely on information available from public sources and information obtained through customer interaction.

12. NON-FACE-TO-FACE BUSINESS RELATIONSHIPS

Non-face-to-face business relationships may carry higher risks. This includes when a Firm establishes business relations and undertakes transactions according to instructions conveyed by customers over the internet, by email, post, fax or telephone.

The measures taken by a Firm to verify an identity in these circumstances will depend on the nature and characteristics of the product or service provided and the customer's risk profile.

Where verification of identity is performed without face-to-face contact, a Firm should make additional checks to manage the risk of impersonation. The additional checks may consist of robust anti-fraud checks that the Firm routinely undertakes as part of its existing procedures, which may include:

- telephone contact with the customer at a residential or business number that can be verified independently;
- confirmation of the customer's address through an exchange of correspondence, site visit or other appropriate method;
- subject to the customer's consent, telephone confirmation of the customer's employment status with his employer at a listed business number of the employer;
- confirmation of the customer's salary details by requiring the presentation of recent bank statements from another bank, where applicable;
- provision of certified identification documents by lawyers or notaries public, or some other suitably qualified professional; or
- requiring the customer to make an initial deposit into the account with the Firm from funds held by the customer in an account with another bank in Qatar.

Firms should note that applications and transactions undertaken across the internet may pose greater risks than other non-face-to-face business that may, taken together, aggravate the ML/TF risks. Examples of those risk factors include:

- the ease of unauthorised access to the facility, across time zones and locations;
- the ease of making multiple fictitious applications without incurring extra cost or the risk of detection;
- the absence of physical documents; and
- the speed of electronic transactions.

13. SOURCE OF WEALTH AND SOURCE OF FUNDS

A Firm should take reasonable steps, consistent with the risk profile of the customer and the nature of the business relationship, to identify the customer's source of wealth and source of funds. If the applicant's risk profile is not low risk, the Firm must verify the source of the applicant's wealth and funds using reliable, independent source documents, data or information, and keep appropriate records of the same.

Source of wealth generally refers to the origin of the customer's and beneficial owner's entire wealth (i.e. total assets). This relates to how the customer and beneficial owner have acquired the wealth, which is not the same as identifying the assets that they own. Source of wealth information should give an indication about the size of wealth the customer and beneficial owner would be expected to have, and how the customer and beneficial owner acquired the wealth. Although the Firm may not have specific information about assets that are not deposited with or processed by the Firm, it may be possible to obtain general information from the customer, commercial databases or other open sources. Examples of appropriate and reasonable means of establishing source of wealth are information and documents such as evidence of title, copies of trust deeds, audited accounts, a copy of a will (in cases where the source of wealth or funds is an inheritance), and conveyancing documents (in cases where the source of wealth or funds is a sale of property), salary details, tax returns and bank statements.

Source of funds refers to the origin of the particular funds or other assets which are used by the customer as part of the business relationship with the Firm (e.g. the amounts being invested, deposited, or wired as part of the business relationship). To minimise the risk that the funds are the proceeds of crime, the Firm should look at the activity that generated the funds and not just identity the Financial Institution from which the funds have been transferred. The type and extent of enquiries required to establish the source of funds will depend on the risk profile of the customer and the nature of the particular transaction.

14. EXTENT OF CDD

The Firm must ensure that the CDD measures taken in respect of a customer are adequate and address the risks presented by the customer and its business relationship with the Firm. The particular CDD steps that a Firm takes will depend upon the risk profile of the customer. Assessment of a customer's risk profile is discussed in detail in a separate guidance paper: "The Risk Based Approach".

Where a customer is assessed as low risk, the Firm may consider implementing a reduced diligence framework or Simplified Due Diligence (SDD). For higher risk customers, the Firm should take more detailed steps to know and understand the customer, or Enhanced Due Diligence (EDD).

15. SIMPLIFIED DUE DILIGENCE (SDD)

If a customer is assessed as low risk, a Firm may decide to conduct SDD. SDD should not be conducted where there is a suspicion of ML or TF. If there is a significant change to a business of a customer subject to SDD, the Firm should review the customer's risk profile, and if necessary, upgrade the CDD carried out to ensure that it is appropriate to the changed circumstances.

Examples of SDD measures include:

- verifying information about the customer by relying on a search of a regulator's public register, if the customer is subject to a statutory licensing and regulatory regime;
- verifying the identity of a shareholder or beneficial owner of a company listed on a stock exchange and subject to disclosure obligations by obtaining information from a public register, from the customer or from other reliable sources;
- verifying a customer or beneficial owner's identity during the establishment of the business relationship;
- adjusting the amount of information required for verification, e.g. relying on one reliable, credible, and independent document or data source only;
- adjusting the quality or source of information e.g. accepting information from the customer rather than an independent source when identifying a beneficial owner;
- adjusting the frequency of CDD reviews of the business relationship;
- adjusting the frequency and intensity of transaction monitoring.

16. ENHANCED DUE DILIGENCE (EDD)

If a customer is assessed as high risk, the Firm must conduct EDD. In addition, the Firm must conduct EDD if a customer has been identified as high risk in the NRA, or in circulators published by NAMLC, or if required by a Competent Authority.

Examples of EDD measures include:

- verification of information by using multiple reliable and independent sources;
- obtaining additional information on a customer (e.g. occupation, amount of assets, information from public databases, internet searches etc.) and more regularly updating the identification data of the customer and beneficial owners;
- obtaining additional information on the intended nature of the business relationship;
- obtaining information on the source of funds or source of wealth of a customer;
- obtaining information about the reasons for proposed transactions or transactions that have already been undertaken;
- requiring that the first transaction to carried out through an account in the customer's name with another bank in Qatar;
- seeking senior management approval to commence or continue a business relationship; and
- enhanced monitoring of the business relationship by increasing the number and timing of controls and selecting particular types or patterns of transactions that need further review.

17. CUSTOMER SCREENING

Customer screening is an important part of a Firm knowing its customer. Screening must be conducted at the commencement of a business relationship and on an ongoing basis.

The primary purpose of customer screening is to ensure that a Firm does not conduct business with people or organisations named on sanctions lists.[1] In addition, Firm should consider checking for other information which may influence a customer's risk profile. For example media reports, credit checks, business information reports etc. may be useful in developing a more complete profile of a customer. Often commercial databases will provide this information in addition to sanctions checking and monitoring.

Economic and trade sanctions have been imposed by countries and international bodies to target some foreign countries, terrorists, drug traffickers and those involved with the proliferation of weapons of mass destruction. Qatar National Terrorist Designation Lists and United Nations sanctions are most relevant to Firms operating in Qatar, but Firms should also be aware of other sanctions which are relevant to their operations and areas of business.

[1] Some jurisdictions have processes that allow Firms to seek permission from government agencies to conduct business with people or organisations named on sanctions lists. However, this topic is beyond the scope of this guidance paper. If this issue applies to a Firm's business, they should obtain legal advice in the relevant jurisdiction.

Qatar National Terrorist Designation Lists are issued by the National Counter Terrorism Committee (NCTC), and can be found on the NCTC website:

https://portal.moi.gov.qa/wps/portal/NCTC/list_main/!ut/p/a1/hY5Nj4IwEIZ_i4dembHi541VAyriR0iEXkzNslhTKLZd9u8vEj3punOaefPMkxcYJMBKXoucW6FKLm83GxwXY-rSwKWhv1jPcbfZLWfu1qcYdRsgbYB-EM59d4WRP4w_GoAG8WAfUMTuf_8HYC3yztAC-Md4CEtguVSntm7qlafeKAems69MZ9r51k18trYyE4IEK6Utl06hhJOr2rlygj-VeeQEo2k8JSiFsceCi_K-fmaWC2le-c_KWEietFAVCV76sg69TucXNkj08A!!/dl5/d5/L2dBISEvZ0FBIS9nQSEh/

United Nations Security Council (UNSC) Resolutions, issued under Chapter VII of the United Nations Charter, are immediately binding on all United Nations member states. Qatar is a member of the United Nations. Accordingly, sanctions imposed by UNSC Resolutions apply to Firms operating in Qatar.

The UNSC administers a list pursuant to UNSC Resolution 1267 (and 1333, 1390, 1455, 1526, 1617 and 1735) which identifies known individuals and entities. This list is updated continuously and amendments are incorporated into the consolidated list which can be found on the United Nations website:

https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/consolidated.xsl

Terrorist screening is not a risk-sensitive due diligence measure and should be carried out irrespective of the risk profile of the customer. Screening is intended to be a preventive measure.

Firms should screen customers against relevant sanctions lists prior to the commencement of a business relationship and throughout the business relationship. Screening should also be conducted, as and when amendments are made to sanctions lists and if there are changes to the customer, such as directors, controllers, major shareholders, company name, etc.

Firms should also have systems in place to detect prohibited transactions (e.g. transactions with entities designated by the NCTC, or UNSC Resolutions, or other relevant sanctions). Transaction screening must occur in real time. [2] Any confirmed name match should be reported promptly to the QFIU and a STR should be filed. The Firm must ensure that it does not tip off the customer. Tipping off is defined in paragraph 22 below.

Performing screening after a business relationship has been established could lead to a breach of legislation in Qatar relating to sanctioned parties. If the Firm becomes aware of any breaches, it must immediately inform the QFIU and the relevant Competent Authority.

[2] NCTC matching names guidance can be found at: http://www.qfcra.com/en-us/whatwedo/AntiMoneyLaundering/Documents/20120130_NCTC_UNSC_guidance.pdf

Firms should put in place policies, procedures, systems and controls (PPSC) that clearly set out:

- the frequency of periodic screening;
- the information sources used by the Firm for screening individuals and entities (including commercial databases used to identify adverse information on individuals and entities);
- the roles and responsibilities of the employees involved in the screening, reviewing and discounting of alerts, maintaining and updating of the various screening databases, and escalating potential matches;
- how potential matches from screening are to be resolved by the Firm's employees, including the process for determining whether a potential match is a false positive or a confirmed match;
- the steps to be taken by the Firm's employees for reporting confirmed matches to the Firm's senior management and to the QFIU and the relevant Competent Authority; and
- the steps to be taken to freeze or restrict access to funds by sanctioned persons.

Identification information of a customer, a connected party of the customer, a natural person appointed to act on behalf of the customer, and a beneficial owner of the customer should be entered into the Firm's customer database for ongoing name screening purposes. This will help the Firm to promptly identify any existing customers who become subject to sanctions after the commencement of the business relationship.

Firms may use automatic screening systems, but must ensure that these systems are fit for the purpose on an ongoing basis.

The level of automation used in the screening process should take into account the nature, size and risk profile of a Firm's business. While an automated system is not a regulatory or legal obligation, Firms with large and complex operations and/or Firms facing high AML/CFT risk, would be expected to have automated systems. A Firm should be aware of any shortcomings in its automated screening systems. In particular, it is important to consider "fuzzy matching" to identify non-exact matches. The Firm should ensure that the fuzzy matching process is calibrated to the risk profile of its business. As application of the fuzzy matching process is likely to result in the generation of an increased number of alerts which have to be checked, the Firm's employees will need to have access to CDD information to enable them to exercise their judgment in identifying potential matches. Records should be kept of screening as set out in paragraph 7 above.

18. TRANSACTION MONITORING

A Firm should have a process to monitor a customer's transactions. The threshold amount and frequency of monitoring are determined by the customer's risk profile and the nature of the business relationship.

Transaction monitoring processes or systems may vary in scope or sophistication (e.g. using manual spreadsheets to complex automated systems). The degree of automation or sophistication of processes and systems depends on the size and complexity of the Firm's operations. Whatever their form, the processes and systems used by the Firm should provide its MLRO, compliance staff and relevant business units with timely information needed to identify, analyse, and effectively monitor customer accounts for ML and TF.

As part of ongoing monitoring, a Firm should pay attention to transaction characteristics, such as:

- the nature of a transaction (e.g. abnormal size or frequency for that customer or peer group);
- whether a series of transactions is conducted with the intent to avoid reporting thresholds (e.g. by structuring an otherwise single transaction into a number of smaller transactions);
- the geographic destination or origin of a payment (e.g. to or from a higher risk country); and
- the parties concerned (e.g. a request to make a payment to or from a person on a sanctions list).

A Firm should make further enquiries when a customer performs frequent and cumulatively large transactions without any apparent or visible economic or lawful purpose. For example, frequent transfers of funds to the same recipient over a short period of time, multiple deposits of cash such that the amount of each deposit is not substantial, but the total of which is substantial. Firms should also monitor transactions with parties in high risk countries or jurisdictions.

In determining what would constitute suspicious, complex, unusually large, or an unusual pattern of transactions, a Firm should consider international typologies and information obtained from law enforcement and other authorities (e.g. FATF and the Egmont Group).

The transaction monitoring processes and systems should enable the Firm to monitor multiple accounts of a customer holistically within a business unit and across business units to identify any suspicious transactions. In addition, Firms should perform trend analyses of transactions to identify unusual or suspicious transactions.

In addition, Firms should have processes to monitor related customer accounts holistically within and across business units, so as to better understand the risks

associated with customer groups, identify potential ML and TF risks and report suspicious transactions.

The factors and thresholds used by a Firm to identify suspicious transactions should be properly documented and independently validated to ensure that they are appropriate to its operations and context. A review should also happen at trigger events e.g. a new product or service is launched, an existing product's key features are changed, an existing product is launched in a new segment (e.g. to non-resident customers, to High Net Worth Individuals, etc.) or in a new geographical area. The product/service/feature should not be rolled out without there being a risk assessment of the ML/TF risk, and not without appropriate testing/calibration of transaction monitoring systems. A Firm should periodically review the appropriateness of the factors and thresholds used in the monitoring process.

19. ONGOING MONITORING

Ongoing monitoring of business relationships with customers is a fundamental feature of an effective AML/CFT risk management framework. Ongoing monitoring should be conducted in relation to all customers, but the Firm may adjust the frequency and extent of monitoring in line with the customer's risk profile. The frequency of CDD review may vary depending on each customer's risk profile. Higher risk customers should be subject to more frequent periodic review.

A key part of ongoing monitoring includes maintaining relevant and up-to-date CDD data, documents and information, so that the Firm can identify changes to the customer's risk profile.

A Firm should obtain updated CDD information (including updated copies of the customer's passport or identity documents if these have expired), as part of its periodic CDD review, or when a trigger event occurs. Examples of a trigger event include:

- a significant transaction takes place;
- a material change occurs in the way the customer's account is operated;
- the Firm's policies, procedures, or standards relating to CDD change materially;
- the Firm becomes aware that it lacks sufficient information about the customer; or
- there is a suspicion of ML or TF.

Where there are indications that the risks associated with an existing business relations may have increased, the Firm should request additional information and conduct a review of the customer's risk profile in order to determine if additional measures are necessary.

20. UNUSUAL CIRCUMSTANCES REQUIRING FURTHER INVESTIGATION

When conducting CDD, Firms should be alert to unusual behaviour by a customer or unusual circumstances that may require further investigation. If the Firm remains suspicious after conducting those investigations, it should consider whether it is appropriate to commence or continue a business relationship. The Firm should also consider whether it is appropriate to file a Suspicious Transaction Report (STR) with the Qatar Financial Information Unit (QFIU). The Firm must ensure that it does not tip off the customer.

Examples of unusual customer behaviour include where the customer:

- is secretive or evasive about who they are, the reason for the transaction, or the source of funds;
- uses an intermediary, or does not appear to be directing the transaction, or appears to be acting as a front for an undisclosed controller or Ultimate Beneficial Owner;
- avoids personal contact without good reason;
- refuses to provide information or documentation, or is unable to provide it or needs to refer to a third party, or the documentation provided is suspicious;
- has criminal associations;
- has an unusual level of knowledge about ML processes; or
- does not appear to have a business association with the other parties to a transaction, but appears to be connected to them.

Examples of unusual circumstances concerning the source of funds include:

- large cash payments;
- unexplained payments from a third party;
- large private funding that does not fit the business or personal profile of the payer;
- loans from non-institutional lenders;
- use of corporate assets to fund private expenditure of individuals; or
- use of multiple accounts or foreign accounts from high risk jurisdictions.

Examples of unusual transaction features include:

- size, nature, frequency, or manner of execution;
- early repayment of mortgages/loans;
- short repayment periods for borrowing;
- an excessively high value is placed on assets/securities;
- it is potentially loss making;
- it unnecessarily incurs penalties;
- involving unnecessarily complicated structures or steps in the transaction;
- repetitive instructions involving common features or parties, or back-to-back transactions with assets rapidly changing value;

- the transaction is unusual for the customer, type of business, or age of the business;
- unexplained urgency, requests for short cuts or changes to the transaction particularly at the last minute;
- use of a Power of Attorney in unusual circumstances;
- no obvious commercial purpose to the transaction; or
- abandoning transactions and/or requests to make payments to third parties or back to source.

21. DETECTING AND REPORTING SUSPICIOUS ACTIVITY AND TRANSACTIONS

Firms must ensure that their PPSC cover the detection of suspicious activity or transactions and associated internal and external reporting.

Officers or employees of a Firm must promptly make a STR to the Firm's MLRO where they know, suspect, or have reasonable grounds to suspect ML or TF, or that funds are any of the following:

- the proceeds of crime; or
- related to terrorism financing; or
- linked or related to, or are to be used for, terrorism, terrorist acts, or by terrorist organisations.

The legal obligation on officers and employees of a Firm to make an internal STR as above applies even where a business relationship or transaction does not proceed.

The MLRO is responsible for receiving, investigating, and assessing internal STRs, and if appropriate, making an external STR to the QFIU and telling the relevant Competent Authority that an STR has been made.

A decision whether or not to submit an STR to the QFIU is the MLRO's responsibility. The MLRO must consider all of the information available, and may submit an STR to the QFIU even when no internal STR has been made. All STRs must be made in good faith.

A Firm must ensure that it does not tip off a customer when it makes an STR.

Detailed guidance and frequently asked questions on STRs is available at the website of the QFIU: www.qfiu.gov.qa.

22. WHAT IS TIPPING OFF?

Tipping off, in relation to an applicant for business or a customer of a Firm, is the unauthorised act of disclosing information that may result in the applicant or customer, or a third party (other than the FIU or the Regulator), knowing or suspecting that the applicant or customer is or may be the subject of:

(i) a suspicious transaction report; or

(ii) an investigation relating to money laundering or terrorism financing; and

(iii) may prejudice the prevention or detection of offences, the apprehension or prosecution of offenders, the recovery of proceeds of crime, or the prevention of money laundering or terrorism financing.

PART 3 – CDD CONDUCTED BY INTRODUCERS, INTERMEDIARIES, AND OTHER THIRD PARTIES

23. RELYING ON CDD CONDUCTED BY THIRD PARTIES - GENERAL

In limited, strictly controlled circumstances, Firms may rely on introducers, intermediaries and other third parties to conduct some elements of CDD or to introduce business to the Firm. However, the Firm and its senior management remain responsible for the proper conduct of CDD and ongoing monitoring for its customers.

24. DEALING WITH A SERIES OR CHAIN OF INTRODUCERS, INTERMEDIARIES OR OTHER THIRD PARTIES

Where the Firm is dealing with a series or chain of introducers, intermediaries, and other third parties, the relevant requirements set out in the paragraphs below must be met by each party in the chain and have all relevant information, and where necessary documents, concerning the ultimate customer.

25. RELYING ON CDD CONDUCTED BY A MEMBER OF THE SAME GROUP

A Firm can rely on CDD conducted by another financial institution in the same group, whether in or outside Qatar, if certain criteria are met. The Firm will not have to conduct the CDD itself or obtain the original documents which the group member obtained when it conducted the CDD.

The criteria that must be met are:

- the group member is regulated and supervised for AML/CFT purposes by a AML/CFT Competent Authority in Qatar or an equivalent regulator in another jurisdiction;
- the group member is subject to the AML/CFT Law or equivalent legislation in another jurisdiction;
- the group member is based, incorporated or otherwise established, in Qatar or a foreign jurisdiction that has an effective AML/CFT regime;
- the group member has provided the Firm with all the CDD information about the customer the Firm would have needed, if it had done the CDD itself (i.e. the relevant customer information, but not necessarily documents – see next point below); and
- the Firm has been provided with, or can immediately obtain from the group member on request, a copy of every CDD document it would need if the Firm had conducted the CDD itself.

Alternatively, the criteria listed above do not need to be met if a Competent Authority, or an AML/CFT regulator in the home jurisdiction of the group member, has determined the following:

- the group applies CDD, record keeping requirements and AML/CFT programmes that are compliant with the AML/CFT Law, the AML/CFT By-Law and another other AML/CFT regulations or rules applicable to the Firm's Qatar operations;
- the group's implementation of these requirements is supervised at a group level by a competent authority; and
- the group's AML/CFT policies adequately mitigate risks related to operations in higher risk countries.

26. RELYING ON CDD CONDUCTED BY AN INTRODUCER

If an Introducer's role is to merely introduce a customer to the Firm, and the Introducer meets certain criteria, then the Firm can rely on the CDD conducted by the Introducer. The Firm will not have to conduct the CDD itself or obtain the original documents which the Introducer obtained when it conducted the CDD.

The criteria that the Introducer must meet are:

- it is regulated and supervised for AML/CFT purposes by a AML/CFT Competent Authority in Qatar or an equivalent regulator in another jurisdiction;
- it is subject to the AML/CFT Law or equivalent legislation in another jurisdiction;
- it is based, incorporated or otherwise established, in Qatar or a foreign jurisdiction that has an effective AML/CFT regime; and
- it is not subject to a secrecy law or anything else that would prevent the Firm obtaining any information or original documentation about the customer that the Firm may need for AML/CFT purposes.

If all of the above criteria are met, the Firm must then ensure that the following conditions are met before it can commence a business relationship with the customer:

- it has received an Introducer's certificate for the customer;
- the Introducer has provided the Firm with all the CDD information about the customer the Firm would have needed, if it had done the CDD itself (i.e. the relevant customer information, but not necessarily documents – see next point below); and
- the Firm has been provided with, or can immediately obtain from the Introducer on request, a copy of every CDD document it would need if the Firm had conducted the CDD itself.

27. RELYING ON CDD CONDUCTED BY AN INTERMEDIARY

An Intermediary is an entity which facilitates a business relationship between the Firm and a customer of the Intermediary. An example of an Intermediary is a fund

manager who has an active, ongoing business relationship with a customer in relation to the customer's financial affairs and holds funds on the customer's behalf.

When an Intermediary introduces a customer to the Firm, the Firm can treat the Intermediary as the Firm's customer, if certain criteria are met. Then the Firm will not need to conduct CDD on the Intermediary's customer, or obtain the original documents which the Intermediary obtained when it conducted the CDD.

The criteria that must be met are:

- the Intermediary is regulated and supervised for AML/CFT purposes by an AML/CFT Competent Authority in Qatar or an equivalent regulator in another jurisdiction;
- the Intermediary is subject to the AML/CFT Law or equivalent legislation in another jurisdiction;
- the Intermediary is based, incorporated or otherwise established, in Qatar or a foreign jurisdiction that has an effective AML/CFT regime;
- the Intermediary has provided the Firm with all the CDD information about the customer the Firm would have needed, if it had done the CDD itself; and
- the Firm has been provided with, or can immediately obtain from the Intermediary on request, a copy of every CDD document it would need if the Firm had conducted the CDD itself.

28. RELYING ON CDD CONDUCTED BY AN AGENT OF THE FIRM

If an agent of a Firm conducts AML/CFT activities on behalf of the Firm, including CDD, the Firm must ensure that the agent complies with:

- the AML/CFT Law and any other relevant AML/CFT legislation; and
- the Firm's AML/CFT policies, procedure, systems and controls.

The Firm must have a system in place to monitor the activities of the agent, including regular monitoring to ensure compliance with the above requirements. Compliance monitoring and the resolution of any issues identified must be documented.

29. RELYING ON CDD CONDUCTED BY A SERVICE PROVIDER UNDER AN OUTSOURCING AGREEMENT WITH THE FIRM

If a Firm outsources any of its AML/CFT functions, including CDD, the Firm and its senior management remain responsible and accountable for ensuring that the AML/CFT Law and other relevant legislation is complied with. The Firm should also seek approval for the outsourcing arrangement from the relevant Competent Authority, if that is required.

The Firm must ensure that the outsourcing third party, and the officers, employees, agents, and contractors of the third party, wherever they are located, comply with:

- the AML/CFT Law and any other relevant AML/CFT legislation or rules; and
- the Firm's AML/CFT policies, procedures, systems, and controls.

The Firm must have a system in place to monitor the activities of the outsourcing third party, including regular monitoring to ensure compliance with the above requirements. Compliance monitoring and the resolution of any issues identified must be documented.

30. RELYING ON CDD CONDUCTED UNDER A CORRESPONDENT BANKING RELATIONSHIP WITH THE FIRM

For information regarding CDD in the context of a correspondent banking relationship, see the separate guidance paper "Correspondent Banking Services".

31. RELYING ON CDD CONDUCTED UNDER A CORRESPONDENT SECURITIES RELATIONSHIP WITH THE FIRM

For Information regarding CDD in the context of a correspondent securities relationship, see the separate guidance paper "Correspondent Banking Services".

APPENDIX 1

Examples of particular CDD information by customer type.

Customer	Example of CDD information
Sole Proprietor	• Full registered business name • Business address or principal place of business • Information about the purpose and intended nature of the business relations with the Firm • Names of all natural persons who act on behalf of the sole proprietor (where applicable) • Name of the sole proprietor • Information about the source of funds • A report of the Firm's visit to the customer's place of business, where the Firm assesses it as necessary • Structure of the sole proprietor's business (where applicable) • Records in an independent company registry or evidence of business registration

Customer	Example of CDD information
Partnerships and unincorporated bodies	• Full name of entity • Business address or principal place of business • Information about the purpose and intended nature of the business relations with the Firm • Names of all natural persons who act on behalf of the entity • Names of all connected parties • Names of all beneficial owners • Information about the source of funds • A report of the Firm's visit to the customer's place of business, where the Firm assesses it as necessary • Ownership and control structure • Records in an independent company registry • Partnership deed • The customer's membership with a relevant professional body • Any association the entity may have with other countries or jurisdictions (e.g. the location of the entity's headquarters, operating facilities, branches, subsidiaries)

Customer	Example of CDD information
Companies	• Full name of entity • Business address or principal place of business • Information about the purpose and intended nature of the business relations with the Firm • Names of all natural persons who act on behalf of the entity • Names of all connected parties • Names of all beneficial owners • Information about the source of funds • A report of the Firm's visit to the customer's place of business, where the Firm assesses it as necessary • Ownership and control structure • Records in an independent company registry • Certificate of incumbency, certificate of good standing, share register, as appropriate • Memorandum and Articles of Association • Certificate of Incorporation • Board resolution authorising the opening of the customer's account with the Firm • Any association the entity may have with other countries or jurisdictions (e.g. the location of the entity's headquarters, operating facilities, branches, subsidiaries)

Customer	Example of CDD information
Public sector bodies, government, state owned companies	• Full name of entity • Nature of entity (e.g. overseas government, treaty organisation) • Business address or principal place of business • Information about the purpose and intended nature of the business relations with the Firm • Name of the home state authority and nature of its relationship with its home state authority • Names of all natural persons who act on behalf of the entity • Names of all connected parties • Information about the source of funds • Ownership and control structure • A report of the Firm's visit to the customer's place of business, where the Firm assesses it as necessary • Board resolution authorising the opening of the customer's account with the Firm

Customer	Example of CDD information
Clubs, Societies and Charities	• Full name of entity • Business address or principal place of business • Information about the purpose and intended nature of business relations with the Firm • Information about the nature of the entity's activities and objectives • Names of all trustees (or equivalent) • Names of all natural persons who act on behalf of the entity • Names of all connected parties • Names of all beneficial owners • Information about the source of funds • A report of the Firm's visit to the customer's place of business, where the Firm assesses it as necessary • Ownership and control structure • Constitutional document • Certificate of registration • Committee/Board resolution authorising the opening of the customer's account with the Firm • Records in a relevant and independent registry in the country of establishment

Customer	Example of CDD information
Trust and Other Similar Arrangements	• Full name of entity • Business address or principal place of business • Information about the nature, purpose and objectives of the entity (e.g. discretionary, testamentary) • Names of all natural persons who act on behalf of the entity • Names of all connected parties • Names of all beneficial owners • Information about the source of funds • A report of the Firm's visit to the customer's place of business, where the Firm assesses it as necessary • Information about the purpose and intended nature of business relations with the Firm • Records in a relevant and independent registry in the country or jurisdiction of constitution • Country or jurisdiction of constitution • Trust deed • Names of the settlors/trustees/beneficiaries or any person who has power over the disposition of any property that is subject to the trust • Declaration of trusts • Deed of retirement and appointment of trustees (where applicable)

RESOURCES

The hyperlinks below are provided for convenience, and may be subject to change without notice by the relevant website owners.

Basel Committee on Banking Supervision
Sound management of risks related to ML and financing of terrorism June 2017
http://www.bis.org/bcbs/publ/d405.pdf

European Supervisory Authorities (Joint Committee of the European Supervisory Authorities)
The Risk Factors Guidelines
June 2017
https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf

European Union
Directive (EU) 2018/843 (5th EU AML Directive)
May 2018
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843

Financial Action Task Force
International Standards on Combating ML and the Financing of Terrorism & Proliferation (The FATF Recommendations)
Updated June 2019
https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

Financial Action Task Force
FATF Methodology for assessing technical compliance with the FATF Recommendations and the effectiveness of AML/CFT Systems (The FATF Methodology)
Updated October 2019
https://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf

Monetary Authority of Singapore
Guidelines to MAS Notice 626 on Prevention of ML and Countering the Financing of Terrorism
April 2015
http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Anti_Money%20Laundering_Countering%20the%20Financing%20of%20Terrorism/Guidelines%20to%20MAS%20Notice%20626%20%20April%202015.pdf

Sound Practices to Counter Proliferation Financing

August 2018
https://www.mas.gov.sg/regulation/guidance/sound-practices-to-counter-proliferation-financing

Guidance on AML/CFT Controls in Trade Finance and Correspondent Banking
October 2015
https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/Guidance-on-AML-CFT-Controls-in-Trade-Finance-and-Correspondent-Banking.pdf

UK Financial Conduct Authority
Financial crime: a guide for firms
April 2015
https://www.handbook.fca.org.uk/handbook/document/FC1_FCA_20150427.pdf

UK HM Treasury & Customs
Your responsibilities under money laundering supervision
June 2017
https://www.gov.uk/guidance/money-laundering-regulations-your-responsibilities

UK Solicitors Regulatory Authority
The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
Updated November 2019
https://www.sra.org.uk/solicitors/guidance/ethics-guidance/the-money-laundering-terrorist-financing-and-transfer-of-funds-information-on-the-payer-regulations-2017/

Warning notice: Money Laundering and terrorist financing
Updated November 2019
https://www.sra.org.uk/solicitors/guidance/warning-notices/money-laundering-and-terrorist-financing--warning-notice/

US Federal Financial Institutions Examination Council
Customer Due Diligence (2018)
2018
https://bsaaml.ffiec.gov/manual/RegulatoryRequirements/02