Anti-Money Laundering and Sanctions Rules and Guidance (AML)

*In this attachment underlining indicates new text and striking through indicates deleted text.

3. INTERPRETATION AND TERMINOLOGY

…

3.2 Glossary for AML

…

3.2.1 The following terms and abbreviations bear the following meanings for the purposes of these Rules.

…

eKYC	Means verification of customer identity by way of electronic means only.
eKYC System	Means the technology and associated processes used to undertake eKYC.
Financial Crime	Includes: (a) fraud or dishonesty; (b) misconduct in or misuse of information relating to a financial market; (c) handling the proceeds of crime; or (d) the financing of terrorism.
Non-Face-to-Face (NFTF)	Where a customer is not physically present for a business operation or transaction with a Relevant Person.

…

4. GENERAL COMPLIANCE REQUIREMENTS

4.1 General requirements

4.1.1 (1) A Relevant Person must establish and maintain effective Anti-Money Laundering policies, procedures, systems and controls to prevent opportunities for money laundering, in relation to the Relevant Person and its activities.

(2) A Relevant Person's Anti-Money Laundering policies, procedures, systems and controls must:

(a) ensure compliance with Federal AML Legislation;

(b) enable suspicious Persons and Transactions to be detected and reported;

(c) ensure the Relevant Person is able to provide an appropriate audit trail of a Transaction; and

(d) ensure compliance with any other obligation in these Rules.

(3) A Relevant Person must take reasonable steps to ensure that its Employees comply with the relevant requirements of its Anti-Money Laundering policies, procedures, systems and controls.

(4) A Relevant Person must review the effectiveness of its Anti-Money Laundering policies, procedures, systems and controls at least annually.

(5) The review process may be undertaken:

(a) internally by its internal audit or compliance function; or

(b) by a competent firm of independent auditors or compliance professionals.

(6) The review process required under Rule 4.1.1(4) must cover at least the following:

(a) a sample testing of customer documentation relevant to an assessment of the adequacy of the customer risk assessment or CDD performed by the Relevant Person;

(b) an analysis of all Suspicious Activity Reports to highlight any area where procedures or training may need to be enhanced; and

(c) a review of the adequacy of the level of responsibility and oversight of the Relevant Person's Governing Body and Senior Management in ensuring the Relevant Person has implemented and maintained adequate controls.

Guidance

Where appropriate, a Relevant Person should incorporate all material risks identified in the business risk assessment, such as a new business practice or introduction of new technology, within scope of the annual review under Rule 4.1.1(4).

…

4.5 Record keeping

4.5.1 A Relevant Person must, where relevant, maintain the following records:

(a) a copy of all documents and information obtained in undertaking initial and on-going CDD or due diligence on business partners;

(b) records, consisting of the original documents or certified copies, in respect of the customer business relationship, including:

(i) business correspondence and other information relating to a customer's account;

(ii) sufficient records of transactions to enable individual transactions to be reconstructed; and

(iii) internal findings and analysis relating to a transaction or any business,

if the transaction or business appears unusual or suspicious, whether or not it results in a Suspicious Activity Report;

(c) Internal Suspicious Activity Report notifications made under Rule 14.2.2;

(d) Suspicious Activity Reports and any relevant supporting documents and information, including internal findings and analysis;

(e) any relevant communications with the FIU;

(f) the documents in Rule 4.6.1; and

(g) any other matter that the Relevant Person is expressly required to record under these Rules,

for at least six years from the date on which the notification or report was made, the business relationship ends or the Transaction is completed, whichever occurs last.

Guidance

A Relevant Person must comply with all applicable Rules on record keeping, regardless of whether or not it is outsourcing an element of its CDD process, see also Rule 9.3. This includes the obligation for the Relevant Person to maintain a copy of all documents obtained during initial and on-going CDD. Where using eKYC for CDD, the Relevant Person should maintain the necessary data concerning biometric authentication.

…

6. BUSINESS RISK ASSESSMENT

6.1 Assessing business AML risks

6.1.1 A Relevant Person must:

(a) take appropriate steps to identify and assess money laundering risks to which its business is exposed, taking into consideration the nature, size and complexity of its activities;

(b) when identifying and assessing the risks in (a), take into account, to the extent relevant, any vulnerabilities relating to:

(i) its type of customers and their activities;

(ii) the countries or geographic areas in which it does business;

(iii) its products, services and activity profiles;

(iv) its distribution channels and business partners;

(v) the complexity and volume of its Transactions;

(vi) the development of new products and business practices including new delivery mechanisms, channels and partners;

(vii) the use of new or developing technologies for both new and pre-existing products and services; and

(c) take appropriate measures to ensure that any risk identified as part of the assessment in (a) is taken into account in its day to day operations and is mitigated, including in relation to:

(i) the development of new products;

(ii) the taking on of new ~~Customers~~ customers; and

(iii) changes to its business profile.

6.1.2 A Relevant Person must use the information obtained in undertaking its business risk assessment to:

(a) develop and maintain its Anti-Money Laundering policies, procedures, systems and controls as required by Rule 6.2.1;

(b) ensure that its Anti-Money Laundering policies, procedures, systems and controls adequately mitigate the risks identified as part of the assessment in Rule 6.1.1;

(c) assess the effectiveness of its Anti-Money Laundering policies, procedures, systems and controls as required by Rule 6.2.1(c);

(d) assist in the allocation and prioritisation of Anti-Money Laundering resources; and

(e) assist in the carrying out of the customer risk assessment under Chapter 7.

6.1.3 Without limiting compliance with Rules 6.1.1 and 6.1.2 a Relevant Person must, prior to launching any new product, service, business practice or using a new or developing technology, take reasonable steps to ensure that it has:

(a) assessed and identified the money laundering risks relating to the product, service, business practice or technology; and

(b) taken appropriate steps to mitigate or eliminate the risks identified under (a).

Guidance

1. Unless a Relevant Person understands the money laundering risks to which it is exposed, it cannot take appropriate steps to prevent its business being used for the purposes of money laundering. Money laundering risks vary from business to business depending on the nature of the business, the type of customers a business has, the nature of the products and services sold, and the geographical operations in which it operates.

2. Using the RBA, a Relevant Person should assess its own vulnerabilities to money laundering and take all reasonable steps to eliminate or manage such risks. The results of this assessment will also feed into the Relevant Person's risk assessment of its ~~Customers~~ customers under Chapter 7.

3. In addition to assessing risk arising from money laundering and terrorist financing,

a business risk assessment should assess the potential exposure of a Relevant Person to other Financial Crime, such as fraud and the theft of personal data. The business risk assessment should also address the Relevant Person's potential exposure to cyber security risk, as this risk may have a material impact on the Relevant Person's ability to prevent Financial Crime.

~~3~~4. A Relevant Person should, prior to launching any new product, service, business practice pay specific attention to assessing the potential for risks associated with ~~money laundering.~~ all applicable aspects of Financial Crime. This is especially important given the innovative nature of any such new offering as the Relevant Person may be less familiar with the functioning of the offering, compared to existing offerings.

~~4~~5. Similarly, in using a new or developing technology, such as those associated with the Regulated Activity of Developing Financial Technology Services within the RegLab or when undertaking NFTF business, a Relevant Person should pay specific attention to assessing the potential for risks associated with ~~money laundering~~ Financial Crime that might arise as a result of implementing that innovative technology. For example, while the use of eKYC Systems may reduce the risk of impersonation fraud at customer on-boarding, NFTF interaction with the customer may increase the risk of Financial Crime after a business relationship has been established, through transaction fraud, money laundering or theft of digitally stored CDD documentation.

6. A business risk assessment under Rule 6.1.1(b) should include assessment of the risks associated with the carrying on of NFTF business, particularly the use of eKYC Systems. The assessment should consider incorporating any relevant mitigation measures identified by the Regulator, a competent authority of the U.A.E., FATF, and any other relevant bodies.

6.2 **Anti-Money Laundering systems and controls**

6.2.2 A Relevant Person must:

(a) establish and maintain effective policies, procedures, systems and controls to prevent opportunities for money laundering in relation to the Relevant Person and its activities;

(b) ensure that its systems and controls in (a):

(i) include the provision to the Relevant Person's Senior Management of regular management information on the operation and effectiveness of its Anti- Money Laundering systems and controls necessary to identify, measure, manage and control the Relevant Person's money laundering risks;

(ii) enable it to determine whether a customer or a Beneficial Owners is a PEP;

(iii) enable the Relevant Person to comply with these Rules and Federal AML Legislation; and

(iv) enable the Relevant Person to comply with the Penal Code of the United Arab Emirates; and

(c) ensure that regular risk assessments are carried out on the adequacy of the Relevant Person's Anti-Money Laundering systems and controls to ensure that they continue to enable it to identify, assess, monitor and manage money laundering risk adequately, and are comprehensive and proportionate to the nature, scale and complexity of its activities.

Guidance

1. In Rule 6.2.1(c) the ~~regularity~~ frequency of risk assessments will depend on the nature, size and complexity of the Relevant Person's business and also on when any material changes are made to its business. The risk assessments should also take into account a range of Financial Crimes, including fraud.

2. The risk assessment under Rule 6.2.1(c) should identify actions to mitigate risks associated with undertaking NFTF business generally, and the use of eKYC specifically. This is because, distinct risks are often likely to arise where business is conducted entirely in an NFTF manner, compared to when the business relationship includes a mix of face-to-face and NFTF interactions. The assessment should make reference to risk mitigation measures recommended by the Regulator, a competent authority of the U.A.E., FATF, and other relevant bodies.

…

8. CUSTOMER DUE DILIGENCE

8.1 Requirement to undertake Customer Due Diligence

…

8.1.2 (1) A Relevant Person must also apply CDD measures to each existing customer under Rules 8.3.1, 8.4.1 or 8.5.1 as applicable:

(a) with a frequency appropriate to the outcome of the risk-based approach in relation to each customer; and

(b) when the Relevant Person becomes aware that any of the circumstances relevant to its risk assessment for a customer has changed.

(2) For the purposes of 8.1.2(1), in determining when it is appropriate to apply CDD measures in relation to existing customers, a Relevant Person must take into account, amongst other things:

(a) any indication that the identity of the customer, or the customer's Beneficial Owners, has changed;

(b) any Transactions that are not reasonably consistent with the Relevant Person's knowledge of the customer;

(c) any change in the purpose or intended nature of the Relevant Person's relationship with the customer; or

(d) any other matter that might affect the Relevant Person's risk assessment

of the customer.

Guidance

1. A Relevant Person should undertake appropriate CDD in a manner proportionate to the customer's money laundering risks. This means that all customers are subject to CDD under Rule 8.3.1. However, for high-risk customers, additional Enhanced Customer Due Diligence measures should also be undertaken under Rule 8.4.1. For customers having a low-risk rating, the requirements under Rule 8.3.1 may be modified according to the assessed risk, in accordance with Rule 8.5.1.

2. The frequency for undertaking CDD for existing customers will be determined by the risk rating assigned to a particular customer. The Regulator expects that customers rated high risk for money laundering should be reviewed more frequently than customers rated lower risk for money laundering.

3. A Relevant Person also needs to know who its customers are to guard against a range of Financial Crime risks, including fraud (particularly impersonation fraud).

…

8.3 Customer Due Diligence requirements

….

8.3.2 (1) For the purposes of Rule 8.3.1(1)(a), a Relevant Person must identify a customer and verify the customer's identity in accordance with this Rule.

(2) If a customer is a natural person, a Relevant Person must ~~obtain and verify information about the person's~~:

(a) obtain and verify information about the person's:

(i) full name (including any alias);

(~~b~~ii) date of birth;

(~~c~~iii) nationality; and

(~~d~~iv) legal domicile~~; and~~.

~~(c)~~(b) obtain the person's current residential address (other than a post office box).

….

(5) If a customer is a trust or other similar Legal Arrangement, the Relevant Person must obtain and verify:

(a) a certified copy of the trust deed or other documents that set out the nature, purpose and terms of the trust or arrangement; and

(b) documentary evidence of the appointment of the trustee or any other

person exercising powers under the trust or arrangement.

Guidance on CDD

1. The information required under 8.3.2(2)(a) and (b) should be obtained through a ~~first-hand inspection~~ review of an original current, valid passport or, where a customer does not own a passport, an official identification document which includes a photograph. For the purposes of Rule 8.2.3(2)(a)(i) and (ii) an official government identification document in digital form and issued by a governmental competent authority is considered valid.

2. A Relevant Person should ensure that any documents used for the purpose of identification are original documents, whichever format they are in, including digital.

3. The verification of a customer's identity, including their address, should be based on official documents. Where that is not possible, a Relevant Person should consider using additional documents or information obtained from different independent sources to verify identity. Any lack of official documents and alternative means of verification should lead the Relevant Person to re-assess the customer's risk classification and the associated level of due diligence to be undertaken.

4. For a customer who is a natural person, a Relevant Person should, to the extent possible, verify the current residential address as a matter of good business practice, for commercial reasons and to help verify the customer's identity. Where a Relevant Person does not verify the current residential address, it should ensure doing so is consistent with its risk-based approach to AML and all applicable rules and laws. The Relevant Person must verify the address of a customer subject to Enhanced Customer Due Diligence under Rule 8.4.1.

~~3~~5. Where personal identity documents, such as a passport, ID card or other identification documentation cannot be ~~obtained~~ reviewed in original form~~, for example because a Relevant Person has no physical contact with the Customer~~, the identification documentation provided should be certified as a true copy of the original document by any one of the following:

   a. a registered lawyer;

   b. a registered notary;

   c. a chartered accountant;

   d. a government ministry;

   e. a post office;

   f. a police officer; or

   g. an embassy or consulate.

   The individual or authority undertaking the certification should be contactable if necessary.

   Where a copy of an original identification document is made by a Relevant Person, the copy should be dated, signed and marked with 'original sighted'.

6. Where a Relevant Person uses eKYC for CDD purposes appropriate measures must be adopted to mitigate the risks that may arise from eKYC procedures and the use of an eKYC System. A Relevant Person must ensure that eKYC is secure and effective, includes an appropriate combination of authentication factors when verifying the identity of the customer and ensure it is at least as stringent as face-to-face CDD. Measures should be in place to verify the authenticity of any official government identification document and the actual customer. A Relevant Person should also apply guidance on technical standards for biometric authentication issued by the Regulator or a competent authority of the U.A.E., as applicable.

7. When employing an eKYC System to assist with CDD, a Relevant Person should:

   a. ensure that it has a thorough understanding of the eKYC System itself and the risks of eKYC, including those outlined by relevant guidance from FATF and other international standard setting bodies;

   b. comply with all the Rules of the Regulator relevant to eKYC including, but not limited to, applicable requirements regarding the business risk assessment, as per Rule 6.1, and outsourcing, as per Rule 9.3.

   c. combine eKYC with transaction monitoring, anti-fraud and cyber-security measures to support a wider framework preventing applicable Financial Crime; and

   d. take appropriate steps to identify, assess and mitigate the risk of the eKYC system being misused for the purposes of Financial Crime.

8. A Relevant Person should take reasonable steps to identify whether a customer has more than one nationality. The existence of dual nationality may be a potential risk factor and should be considered as such in the customer risk assessment required by Rule 7.1.2.

….

8.3.6 (1) For the purposes of Rule 8.3.1(1)(b), a Relevant Person must identify the Beneficial Owners of a customer that is a foundation or other Legal Arrangement similar to a foundation in accordance with this Rule.

….

(4) Where any of the persons identified under (2)(a) to (~~e~~d) are a Body Corporate or Partnership, the Relevant Person must identify the Beneficial Owners of Body Corporate or Partnership in accordance with Rule 8.3.3 and Rule 8.3.4.

Guidance on verification of the identity of Beneficial Owners

1. In determining whether an individual meets the definition of Beneficial Owners regard should be had to all the circumstances of the case, in particular the size of an individual's legal engagement or beneficial ownership in a Transaction.

2. For a retail investment fund that is widely-held and where the investors invest via pension contributions, the Regulator would not expect the manager of the

fund to look through to any underlying investors where there are none with any material control or ownership of the fund. However, for a closely-held fund with a small number of investors, each having a large shareholding or other interest, the Regulator would expect a Relevant Person to identify and verify each of the Beneficial Owners, depending on the risks identified as part of its risk-based assessment of the customer. For a corporate health policy with defined benefits, however, the Regulator would not expect a Relevant Person to identify the Beneficial Owners.

3. An eKYC System may be used as part of the identification and verification of Beneficial Owners. When determining whether to use an eKYC System to assist in the CDD of a Beneficial Owner, a Relevant Person should establish if the eKYC System used allows it to comply fully with the relevant Rules in relation to CDD.

…

8.4 Enhanced Customer Due Diligence

8.4.1 Where a Relevant Person is required to undertake Enhanced CDD, having assigned a customer a high risk rating or it or its Beneficial Owners is a PEP, then, in addition to CDD under Rule 8.3.1, it must:

…

(e) obtain the approval of Senior Management to commence a business relationship with the customer; ~~and~~

(f) require the first payment to be carried out through an account in the customer's name with a financial institution that is subject to money laundering regulation and supervision in a jurisdiction that has standards equivalent to those set out in the FATF Recommendations~~.~~; and

(g) for a customer who is a natural person, verify the current residential address (other than a post office box).

…

9. ANTI-MONEY LAUNDERING COMPLIANCE AND THIRD-PARTIES

…

9.3 Outsourcing and agents

9.3.1 A Relevant Person which outsources any one or more elements of its CDD to a service provider (including those within its Group) remains responsible for compliance with, and liable for any failure to meet, such obligations.

~~**Guidance**~~

9.3.1A Prior to appointing ~~an outsourced~~ a service provider to undertake CDD, a Relevant Person ~~should~~ must undertake ~~due diligence~~ an initial assurance assessment to ~~assure itself of~~ evaluate the suitability of the ~~outsourced~~ service provider and ~~should~~ must ensure that the ~~outsourced~~ service provider's obligations are clearly

documented in a binding agreement.

9.3.1B After engaging a service provider the Relevant Person must undertake periodic assurance assessments to ensure that the services provided meet the obligations recorded in the binding agreement and allow it to meet all the requirements that it is subject to.

Guidance

1. A Relevant Person's use of a service provider's eKYC System (enabling a Relevant Person to undertake eKYC) constitutes outsourcing for the purposes of Rule 9.3.1.

2. When undertaking an assurance assessment of an eKYC System for the purpose of Rule 9.3.1A, a Relevant Person should seek to establish that the eKYC System is reliable and independent, and allows the Relevant Person to comply with all applicable Rules of the Regulator. In addition, a Relevant Person should consider applying guidance on assurance standards issued by the Regulator, competent U.A.E. authorities, FATF, and other relevant standard setting bodies.

3. In limited circumstances, a Relevant Person may place reliance on the assurance assessment of the eKYC System conducted entirely by another entity. Such circumstances comprise the following:

    a. Where an assurance assessment of the eKYC System has been undertaken by a Related entity and specifically addresses the Rules and Regulations applicable to the Relevant Person. In such circumstance s, the Relevant Person remains responsible for the eKYC System' s compliance with applicable Rules and Laws and it should maintain a copy of the assessment.

    b. Where the eKYC System has been authorised by a competent authority of the U.A.E. or a competent authority in a jurisdiction with Anti Money Laundering laws equivalent to the U.A.E. In such circumstances, the eKYC system should be authorised for use in CDD. Further, the Relevant Person should undertake its own review to ensure that any use of the relevant eKYC System is appropriate and enables compliance with all Rules and Regulations applicable to the Relevant Person.

    c. Where a Relevant Person chooses to employ a third party to assist in its own assurance assessment of the eKYC System, It should ensure that a competent and independent firm with relevant expertise and resources be employed. The Relevant Person remains wholly responsible for the eKYC System' s compliance with, and any failure to meet, the Rules and Regulation applicable to the Relevant Person.

4. In complying with Rule 9.3.1, a Relevant Person should ensure that the service provider can be replaced with minimal disruption in the event the outsourcing arrangement is terminated.

5. An Authorised Person is also required to comply with the outsourcing obligations in GEN 3.3.31 and 3.3.32 and PRU 6.8. A Recognised Body is

also required to comply with the outsourcing obligations in MIR 2.14.

…

14. SUSPICIOUS ACTIVITY REPORTS

…

14.2 Internal reporting requirements

….

14.2.3 A Relevant Person must have policies and procedures to ensure that disciplinary action can be taken against any Employee who fails to make such a report.

Guidance

1. Circumstances that might give rise to suspicion or reasonable grounds for suspicion of money laundering include:

…

2. CDD measures form the basis for recognising suspicious activity. Sufficient guidance must therefore be given to the Relevant Person's Employees to enable them to form a suspicion or to recognise when they have reasonable grounds to suspect that money laundering or terrorist financing is taking place. This should involve training that will enable relevant Employees to seek and assess the information that is required for them to judge whether a Person is involved in suspicious activity related to money laundering or terrorist financing.

3. Where appropriate, a Relevant Person should also utilise the methods described in paragraph 1 above to detect a range of Financial Crimes, including fraud. Bearing in mind the evolving nature of Financial Crime and the methods used to further it, a Relevant Person should apply best practice when determining which behaviours would constitute as suspicious and what measures are required to detect suspicious transactions. Such practices may include, but are not limited to, incorporating the analysis of customer behaviour metrics into the monitoring of suspicious transactions.

~~3.~~4. The requirement for Employees to notify the Relevant Person's MLRO should include situations when no business relationship was developed because the circumstances were suspicious.

~~4.~~5. A Relevant Person may allow its Employees to consult with their line managers before sending a report to the MLRO. The Regulator would expect that such consultation does not prevent making a report whenever an Employee has stated that he has knowledge, suspicion or reasonable grounds for knowing or suspecting that a Person may be involved in money laundering. Whether or not an Employee consults with his line manager or other Employees, the responsibility remains with the Employee to decide for himself whether a notification to the MLRO should be made.

~~5.~~6. An Employee, including the MLRO, who considers that a Person is engaged in or engaging in activity that he knows or suspects to be suspicious would not be expected to know the exact nature of the criminal offence or that the particular funds were definitely those arising from the crime of money

laundering or terrorist financing.

~~6.~~7. A Transaction that appears unusual is not necessarily suspicious. Even ~~Customers~~ customers with a stable and predictable Transaction profile will have periodic Transactions that are unusual for them. Many ~~Customers~~ customers will, for perfectly good reasons, have an erratic pattern of Transactions or account activity. So the unusual is, in the first instance, only a basis for further inquiry, which may in turn require judgement as to whether it is suspicious. A Transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report it then arises.

~~7.~~8. Effective CDD measures may provide the basis for recognising unusual and suspicious activity. Where there is a customer relationship, suspicious activity will often be one that is inconsistent with a customer's known legitimate activity, or with the normal business activities for that type of account or customer. Therefore, the key to recognising "suspicious activity" is knowing enough about the customer and the customer's normal expected activities to recognise when their activity is abnormal.

~~8.~~9. A Relevant Person may consider implementing policies and procedures whereby disciplinary action is taken against an Employee who fails to notify the Relevant Person's MLRO.

…