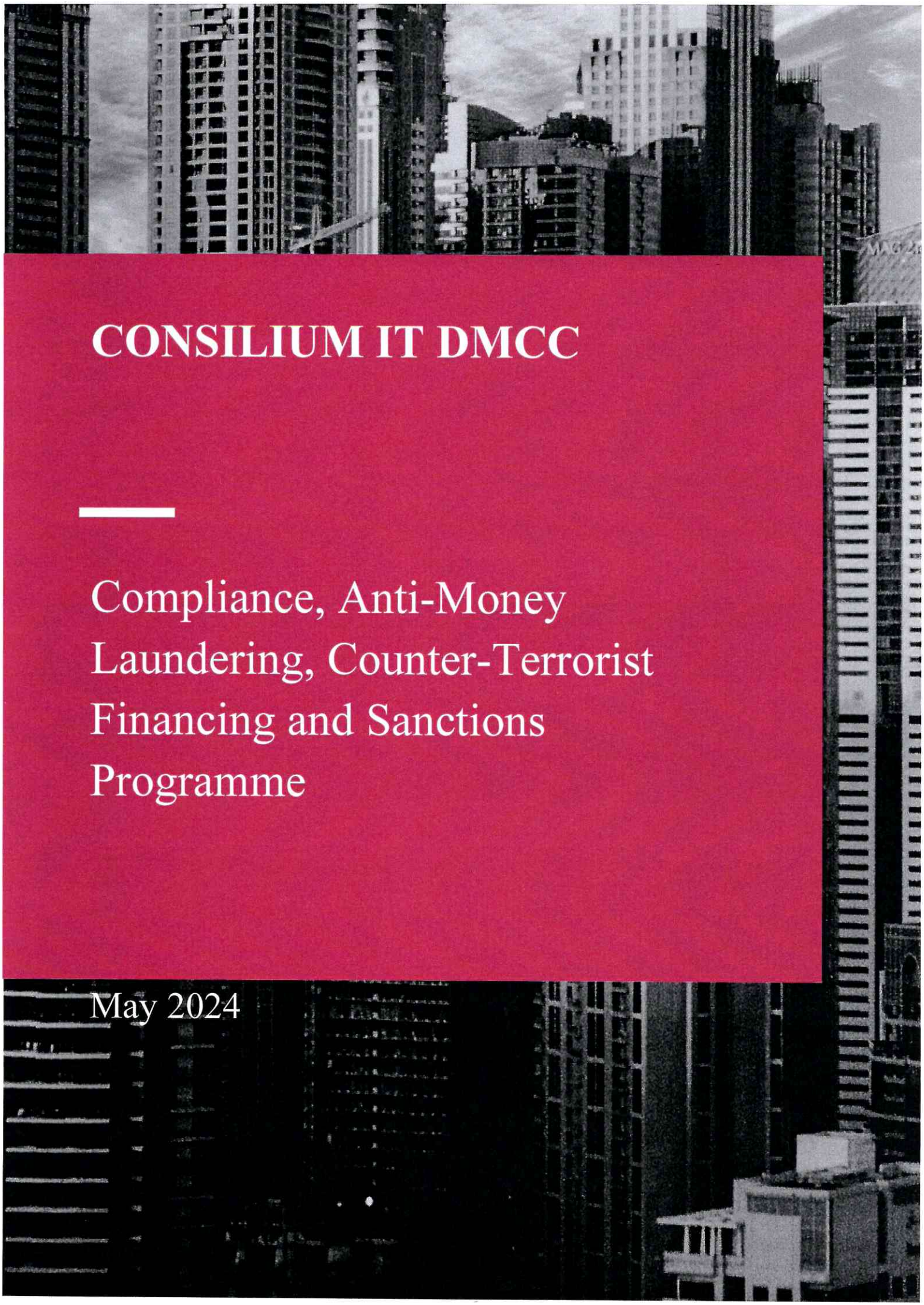

CONSILIUM IT DMCC

Compliance, Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Programme

May 2024

TABLE OF CONTENTS

3

1. OVERVIEW AND PURPOSE OF THE PROGRAMME

Guidance

In this Programme, for simplicity, a reference to "money laundering" also includes terrorist financingand the financing of illegal organisations.

Overview of the DMCC's AML regime

The DMCC is governed by two separate and complementary regimes in relation to AML regulation:

a. The Federal regime:

- Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing ofTerrorism and Illegal Organisations
- Federal Law No. 7 of 2014 on Combating Terrorism Offences
- Cabinet Decision No. 10 of 2019 on the Implementing Regulations of Federal Law No. 20 of 2018
- Cabinet Decision No. 20 of 2019 regarding Terrorism Lists Regulation and Implementation of UN

Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing andProliferation of Weapons of Mass Destruction, and Related Resolutions;
- Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of UN SecurityCouncil Resolutions on the Suppression and Combating of Terrorism, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions.
- Cabinet Decision No. (58) of 2020 Regulating the Beneficial Owner Procedures; and

b. The DMCC regime:

the Dubai Multi Commodities Centre Authority (DMCC), established pursuant to Law No. 4 of 2001 and by virtue of Decision No. 4 of 2002, each issued in the Emirate of Dubai, is the authority which has governance over the DMCC Free Zone.

On the 30the of June 2019 DMCCA enacted the AML/CFT Guidelines for Financial Institutions and Designated Non-Financial Businesses and Professions.

Notwithstanding these Guidelines are not mandatory rules for **CONSILIUM IT DMCC** (as thecompany is not the financial institution) these recommendations are implemented in this Programme.

Purpose of the AML Programme

The AML Programme cannot be read in isolation from local and international legislation and best practice.

This is particularly relevant when considering the list of persons and terrorist organisations issued underCabinet Decision No. 20 of 2019 and the United Nations Security Council Resolutions (UNSCRs).

The U.A.E. criminal law

The U.A.E. criminal law applies in the DMCC and, therefore, persons in the DMCC must be aware of their obligations in respect of the criminal law as well as these Rules. Relevant U.A.E. criminal laws include Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations, Federal Law No. 7 of 2014 on Combating Terrorism Offences and the Penal Code of the U.A.E

Under Federal AML legislation a Person can be found liable for a crime such as:

a. money laundering;

b. financing terrorism;

c. financing illegal organisations;

d. 'tipping off';

e. violation of sanctions;

f. failure to declare currency or precious metals brought into or taken out of the U.A.E.

The U.A.E Central Bank has the power under Federal AML legislation to freeze funds or other assets suspected of relating to money laundering, terrorist financing or the financing of illegal organisations. Other Federal authorities also have powers to apply for the freezing or confiscation of funds or other assets that have been used for such purposes.

Financial Action Task Force

The Financial Action Task Force (FATF) is an inter-governmental body whose purpose is the development and promotion of international standards to combat money laundering and terrorist financing.

The U.A.E., as a member of the United Nations, is required to comply with sanctions issued and passed by the United Nations Security Council (UNSC). These UNSC obligations apply in the DMCC and their importance is emphasised by specific obligations contained in this Programme requiring Company to establish and maintain effective systems and controls to comply with UNSC sanctions and resolutions.

The FATF has issued guidance on a number of specific UNSC sanctions and resolutions regarding the countering of the proliferation of weapons of mass destruction. Such guidance has been issued to assist in implementing the targeted financial sanctions and activity based financial prohibitions. This guidance can be found on the FATF website http://www.fatf- gafi.org

The Wolfsberg Group is an association of thirteen global banks which aims to develop frameworks and guidance for the management of financial crime risks. The CBDDQ aims to set an enhanced and reasonable standard for cross-border and/or other higher risk Correspondent Banking Due Diligence, reducing to a minimum any additional data requirements, as per the Wolfsberg definition and current FATF Guidance. The Wolfsberg Group is is an association of thirteen global banks which aims to develop frameworks and guidance for the management of financial crime risks.

2. INTERPRETATION AND TERMINOLOGY

2.1 Interpretation

2.1.1 A reference in this Programme to "money laundering" in lower case includes a reference toterrorist financing and the financing of illegal organisations, unless the context implies otherwise.

2.2 Glossary for AML

2.2.1 In this Programme, the terms and abbreviations listed in the table below have the followingmeanings:

AML	Means either "anti-money laundering" or Anti-Money Laundering, Counter-Terrorist Financing and Sanctions, depending on the context.
Beneficial Owner	The natural person who directly or indirectly owns equity shares or shares of 25% or more or exercises effective ultimate control over a client or the natural person on whose behalf a transaction is being conducted or, the natural person who exercises effective ultimate control over a legal person or legal arrangement.
Body corporate	Any body corporate, including a limited liability partnership, whether constituted under the law of the DMCC, an Emirate, the State or any other country or territory.
Cabinet DecisionNo. 10 of 2019	Means Federal Cabinet Decision No. 10 of 2019 on the Implementing Regulations of Federal Law No. 20 of 2018.
Cabinet DecisionNo. 20 of 2019	Means Federal Cabinet Decision No. 20 of 2019 regarding Terrorism Lists Regulation and Implementation of UN SecurityCouncil Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing and Proliferation of Weapons of Mass Destruction, and Related Resolutions.
Customer Due Diligence (CDD)	The process of identifying or verifying the information of a Customer or Beneficial owner, whether a natural or legal personor a legal arrangement, and the nature of its activity and the purpose of the business relationship and the ownership structure and control over it.

Company	**CONSILIUM IT DMCC** Registration Certificate № DMCC189560 License DMCC-800200 on the 11/01/2021 by the Dubai MultiCommodities Centre Authority (DMCCA) Address: Unit No: 3O-01-BA1132 Jewellery & Gemplex 3, Plot No: DMCC-PH2-J&GPlexS Jewellery & Gemplex, Dubai, United Arab Emirates
CFT	Means Combating the financing of terrorism.
Customer	Unless otherwise provided, means: the legal entity to which Company is going to render or rendersthe services according to legal agreement.
MCC	the Dubai Multi Commodities Centre
DMCCA	the Dubai Multi Commodities Centre Authority, established pursuant to Law No. 4 of 2001 and by virtue of Decision No. 4 of2002, each issued in the Emirate of Dubai, which authority has governance over the DMCC Free Zone as a Competent Authority.
FATF	Means the Financial Action Task Force.
FATF Recommendations	Means the publication entitled the "International Standards onCombatting Money Laundering and the Financing of Terrorism and Proliferation" as published and amended from time to time by FATF.
Federal AML legislation	Means all U.A.E Federal Laws and their implementing regulations relating to money laundering, terrorist financing and the financing of illegal organizations, as well as sanctions compliance, including Federal Law No. 20 of 2018, Federal Law No. 7 of 2014, Cabinet Decision No. 10 of 2019 and Cabinet Decision No. 20 of 2019.
Federal Law No. 20of 2018	Means U.A.E Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations.
Federal Law No. 7of 2014	Means U.A.E Federal Law No. 7 of 2014 on Combating TerrorismOffences.
FIU	The Financial Intelligence Unit of the Central Bank of the U.A.E.

Regulated Financial Institutions	Banks, finance companies, currency exchange offices, financialand monetary brokers or any other financial institution licensed by the Central Bank or Supervisory Authority to operate in the State, whether they were publicly or privately owned. Means a regulator of financial services activities established in a jurisdiction other than the DMCC.
Funds	Assets in whatever form, tangible or intangible, movable or immovable including national currency, foreign currencies, documents or notes evidencing the ownership of those assets orassociated rights in any forms including electronic or digital forms or any interests, profits or income originating or earned from these assets.
Governing Body	Means the board of directors, partners, committee ofmanagement or other governing body.
High risk (prohibited) jurisdictions	The Company will not process or accept customers incorporatedor operating in the below jurisdictions: Afghanistan, Central African Republic, Democratic Republic of the Congo, Iran, Iraq,Libya, Mali, Moldova, North Korea, Somalia, Saudi Arabia, Sudan, South Sudan, Syria, Yemen.
IMF	The International Monetary Fund.
International Organization	Means an organization established by formal political agreement between member countries, where the agreement has the status ofan international treaty, and the organization is recognized in the law of countries which are members.
MENAFATF	The Middle East and North Africa Financial Action Task Force.
MLRO	Means the person appointed by the Company as a MoneyLaundering Reporting Officer
RCS	Internally developed Risk Control System (RCS), that covers 24/7 Sanction, PEP Screening as well as prevention of fraud scenarios and

	detection of suspicious transactions. RCS collects and analyzes such data as IP address, operation type, Customer ID etc.
Money laundering	Means engaging in any of the following acts willfully, havingknowledge that the funds are the proceeds of a felony or a misdemeanor (i.e., a predicate offence): - Transferring or moving proceeds or conducting any transactionwith the aim of concealing or disguising their Illegal source; - Concealing or disguising the true nature, source or location ofthe proceeds as well as the method involving their disposition, movement, ownership of or rights with respect to said proceeds; - Acquiring, possessing or using proceeds upon receipt; - Assisting the perpetrator of the predicate offense to escapepunishment.
OECD	The Organization for Economic Co-operationand Development.
Politically Exposed Person (PEP)	Means a natural person (and includes, where relevant, a family member or close associate) who is or has been entrusted with a prominent public function, whether in the State or elsewhere, including but not limited to, a head of state or of government, senior politician, senior government, judicial or military official, ambassador, senior person in an International Organisation, senior executive of a state owned corporation, an important political party official, or a member of senior management or an individual who has been entrusted with similar functions such as a director or a deputy director.This definition does not include middle ranking or more junior individuals in the above categories.
Senior management	Means: In relation to a Company every member of the Company's executive management and includes: In relation to a customer that is a body corporate, every memberof the body corporate's Governing Body and the person or personswho control the day-to-day operations of the body corporate, including its senior executive officer, chief operating officer and chief financial officer.
Shell Bank	A bank that has no physical presence in the country in which it is incorporated or licensed and which is not affiliated with a regulated financial group that is subject to effective consolidated supervision.

Source of funds	Means the origin of funds which relate to a transaction or service and includes how such funds are connected to the source of wealthof a customer or Beneficial Owner.
Source of wealth	Means how the global wealth or net worth of a customer orBeneficial Owner is or was acquired or accumulated.
State	Means The United Arab Emirates (the U.A.E.)
Suspicious ActivityReport (SAR)	Means a report regarding suspicious activity (including a suspicious transaction) made to the FIU under Federal Law No. 20 of 2018 and Cabinet Decision No. 10 of 2019.
Transaction	All disposal or use of Funds or proceeds including for example: deposit, withdrawal, conversion, sale, purchase, lending, swap,mortgage, and donation.

3. RISK-BASED APPROACH

3.1. The Company must:

(a) assess its AML risks under this Programme by reviewing the risks to which the person is exposed as a result of the nature of its business, customers, products, services, and any other matters which are relevant in the context of money laundering and then adopting a proportionate approach to mitigate those risks; and

(b) ensure that, when undertaking any risk-based assessment for the purposes of complying with a requirement of this Programme, such assessment is:

(i) objective and proportionate to the risks;

(ii) based on reasonable grounds;

(iii) properly documented; and

(iv) reviewed and updated at appropriate intervals.

4. BUSINESS RISK ASSESSMENT

4.1. Assessing business AML risks

4.1.1 The Company 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, 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 new business practices, including new delivery mechanisms, channels and

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

(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, including in relation to:

(i) the development of new products, business practices and technologies

(ii) the taking on of new customers; and

(iii) changes to its business profile.

4.1.2 New products, business practices and technologies

(1) This Rule applies in relation to:

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

(b) the use of new or developing technologies for both new and existing products.

(2) The Company must take reasonable steps to ensure that it has:

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

(b) taken appropriate steps to manage and mitigate the risks identified under (a), before it launches or uses the new product, practice or technology.

4.2 AML systems and controls

4.2.1 The Company must:

(a) establish and maintain effective procedures, systems and controls to prevent opportunities formoney laundering in relation to the Company and its activities;

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

(i) include the provision to the Company's senior management of regular management informationon the operation and effectiveness of its AML systems and controls necessary to identify, measure, manage and control the Company's money laundering risks;

(ii) enable it to determine:

(A) whether a customer or a Beneficial Owner is a Politically Exposed Person (PEP);

(iii) enable the Company to comply with these Programme and Federal AML legislation; and

(c) ensure that regular risk assessments are carried out on the adequacy of the Company's AML 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.

5. CUSTOMER RISK ASSESSMENT

5.1. Assessing customer AML risks

(1) The Company must:

(a) undertake a risk-based assessment of every customer; and

(b) assign the customer a risk rating proportionate to the customer's money laundering risks.

(2) The customer risk assessment in (1) must be completed prior to undertaking Customer DueDiligence for new customers, and whenever it is otherwise appropriate for existing customers.

(3) When undertaking a risk-based assessment of a customer under (1)(a) The Company must:

(a) identify the customer and any Beneficial Owner;

(b) obtain information on the purpose and intended nature of the business relationship;

(c) obtain information on, and take into consideration, the nature of the customer's business;

(d) take into consideration the nature of the customer, its ownership and control structure, and its Beneficial Ownership (if any);

(e) take into consideration the nature of the customer business relationship with the Company;

(f) take into consideration the customer's country of origin, residence, nationality, place ofincorporation or place of business;

take into consideration the relevant product, service or transaction.

5.2. Factors that may indicate higher money laundering risk

(1) When assessing if there is a high risk of money laundering in a particular situation, the Companymust take into account, among other things:

(a) customer risk factors, including whether:

(i) the business relationship is conducted in unusual circumstances;

(ii) the customer is resident, established or registered in a geographical area of high risk (as set outin paragraph (c));

(iii) the customer is a legal person or legal arrangement that is a vehicle for holding personal assets;

(iv) the customer is a company that has nominee shareholders or shares in bearer form;

(v) the customer is a business that is cash intensive, such as a business that receives a majority of itsrevenue in cash; and

(vi) the corporate structure of the customer is unusual or excessively complex given the nature of thebusiness;

(b) product, service, transaction or delivery channel risk factors, including whether:

(i) the service involves private banking;

(ii) the product, service or transaction is one that might favour anonymity;

(iii) the situation involves non face-to-face business relationships or transactions, without certainsafeguards, such as electronic signatures;

(iv) payments will be received from unknown or unassociated third parties;

(v) new products and new business practices are involved, including new delivery mechanisms orthe use of new or developing technologies for both new and pre-existing products; and

(vi) the service involves the provision of nominee directors, nominee shareholders or shadowdirectors, or the formation of companies in another country; and

(c) geographical risk factors, including:

(i) countries identified in reports by credible sources, such as mutual evaluations, detailedassessment reports or follow-up reports, as:

(A) not having effective systems to counter money laundering; or

(B) not implementing requirements to counter money laundering that are consistent with FATFRecommendations;

(ii) countries identified by credible sources as having significant levels of corruption or other criminal activity, such as terrorism, money laundering or the production and supply of illicit drugs;

(iii) countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations or the State;

(iv) countries providing funding or support for terrorism; and

(v) countries that have organisations operating within their territory that have been designated by the State, other countries or International Organisations as terrorist organisations.

(2) For the purposes of (1)(c), a credible source includes, but is not limited to, FATF, the IMF, the World Bank, the OECD and other International Organisations.

(3) When assessing the risk factors referred to in (1), Company must bear in mind that the presenceof one or more risk factors may not always indicate a high risk of money laundering in a particular situation.

5.2.1. Factors that may indicate lower money laundering risk

(1) When assessing if there is a low risk of money laundering in a particular situation, the Companymust take into account, among other things:

(a) customer risk factors, including whether the customer is:

(i) a public body or a publicly owned enterprise;

(ii) resident, established or registered in a geographical area of lower risk;

(iii) a Regulated Financial Institution that is subject to regulation and supervision, including AML regulation and supervision, in a jurisdiction with AML regulations that are equivalent to the standards set out in the FATF Recommendations;

(iv) a Subsidiary of a Regulated Financial Institution, if the law that applies to the Parent ensures that the Subsidiary also observes the same AML standards as its Parent;

(v) a company whose Securities are listed by Regulated Exchange and which is subject to disclosure obligations broadly equivalent to those set out in the Markets Rules;

(vi) a law firm, notary firm or other legal business that carries on its business in or from the DMCC; and

(vii) an accounting firm, insolvency firm, Registered Auditor or other audit firm that carries on its business in or from DMCC;

(b) product, service, transaction or delivery channel risk factors, including whether the product or service is:

(c) (i) a product where the risks of money laundering are adequately managed by other factors such as transaction limits or transparency of ownership; and geographical risk factors, including whether:

(i) a country has been identified by credible sources as having effective systems to counter money laundering;

(ii) a country is identified by credible sources as having a low level of corruption or other criminal activity, such as terrorism, money laundering, or the production and supply of illicit drugs; and

(iii) on the basis of reports by credible sources, such as mutual evaluations, detailed assessment reports or follow-up reports, a country:

(A) has requirements to counter money laundering that are consistent with the FATF Recommendations; and effectively implements those Recommendations.

(2) For the purposes of (1)(c), a credible source includes, but is not limited to, FATF, the IMF, the World Bank, the OECD and other International Organisations.

(3) When assessing the risk factors referred to in (1), Company must take into consideration that the presence of one or more risk factors may not always indicate a low risk of money laundering in a particular situation.

5.3. Business relationship not to be established if ownership arrangements prevent identification of beneficial owners

The Company must not establish a business relationship with the customer which is a legal person if theownership or control arrangements of the customer prevent the Company from identifying one or more of thecustomer's Beneficial Owners.

5.4. Shell Banks

The Company must not establish or maintain a business relationship with a Shell Bank.

5.5. Anonymous or fictitious accounts

The Company must not establish or maintain an anonymous account, an account in a fictitious name, or a nominee account which is held in the name of one person but which is controlled by or held for the benefitof another person whose identity has not been disclosed to the Company.

6 CUSTOMER DUE DILIGENCE

6.1 Requirement to undertake customer due diligence

(1) The Company must:

(a) undertake Customer Due Diligence for each of its customers before the conclusion of legalagreement and prossessing live transactions; and

(b) in addition to (a), undertake Enhanced Customer Due Diligence in respect of any customer ithas assigned as high risk.

(2) The Company may undertake Simplified Customer Due Diligence by modifying Customer DueDiligence for any customer it has assigned as low risk.

6.2 Timing of customer due diligence

6.2.1. (1) The Company must also undertake appropriate Customer Due Diligence if, at any time:

(a) in relation to an existing customer, it doubts the veracity or adequacy of documents, data orinformation obtained for the purposes of Customer Due Diligence;

(b) it suspects money laundering in relation to a customer; or

(c) there is a change in risk-rating of the customer, or it is otherwise warranted by a change incircumstances of the customer.

6.3 Customer due diligence requirements

6.3.1 Undertaking customer due diligence

(1) In undertaking Customer Due Diligence the Company must:

(a) identify the customer and verify the customer's identity;

(b) identify any Beneficial Owners of the customer and take reasonable measures to verify the identity of theBeneficial Owners, so that the Company is satisfied that it knows who the Beneficial Owners are;

(c) visit site (if applicable) to comply with quality assurance

(d) if the customer is a legal person or legal arrangement, take reasonable measures to understand the nature of the customer's business and its ownership and control structure; and

(e) undertake on-going due diligence of the customer business relationship.

(2) If a person ("A") purports to act on behalf of the customer, the Company:

(a) verify that A is authorised to act on the customer's behalf; and

(b) identify A and verify A's identity.

(3) The verification under (1) and (2) must be based on reliable and independent source documents,data or information.

6.3.2 Identifying and verifying the customer

(1) The Company must identify a customer and verify the customer's identity in accordance withthis Programme.

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

(a) full name (including any alias);

(b) date of birth;

(c) nationality;

(d) legal domicile; and

(e) current residential address (other than a post office box)

(f) another contact details (e-mail, phone number).

(3) If a customer is a body corporate, the Company must obtain and verify:

(a) the full name of the body corporate and any trading name;

(b) the address of its registered office and, if different, its principal place of business;

(c) the date and place of incorporation or registration;

(d) a copy of the certificate of incorporation or registration;

(e) the articles of association or other equivalent governing documents of the body corporate; and

(f) the full names of its senior management

(g) valid commercial or professional license (if applicable).

(4) If a customer is an express trust or other similar legal arrangement, the Company must obtain andverify:

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

(b) documentary evidence of the appointment of the trustee or any other person exercising powersunder the trust or arrangement.

6.3.3 Identifying and verifying beneficial owners: body corporate

(1) If a customer is a body corporate, the Company must identify and verify the Beneficial Owners.

(2) The Company must identify:

(a) the natural persons who ultimately have a controlling 25% or more ownership interest in the bodycorporate, whether legal or beneficial, direct or indirect; If two or more natural persons jointly own or control a ratio of capital in the Legal Person, all of them shall be deemed as jointly owners or controllers ofsuch ratio and

(b) if there is any doubt about whether the natural persons identified under

(a) exert control through ownership interests, or if no natural person exerts control throughownership interests, the natural persons exercising control of the body corporate through othermeans.

6.3.4 The Company is not required to identify and verify Beneficial Owner if the customer is either:

(a) a body corporate that:

(i) has its Securities listed by Regulated Exchange; and

(ii) is subject to disclosure requirements which ensure that adequate information about its business,structure and beneficial ownership is publicly available; or

(b) a majority-owned subsidiary of a body corporate referred to in (a).

If, after all reasonable means have been taken, no natural person is identified as an ultimate Beneficial Owner, or there is reasonable doubt that any natural person identified as an ultimate Beneficial Owner is the true Beneficial Owner in the Legal Person; then the natural person who controls the Legal Personby other means of control shall be deemed as the Beneficial Owner. Where no natural person is identified; then the natural person who holds the position of a higher management official shall be deemed as the Beneficial Owner.

6.3.5. Identifying and verifying beneficial owners: trusts and similar arrangements

(1) The Company must identify:

(a) for a trust, the settlor, trustee, protector, enforcer, beneficiaries and any other natural person who exercises ultimate effective control over the trust. this shall not apply to the licensed or registered Legal Persons in the State that are owned by a company listed on a recognized stock exchange subject to disclosure requirements which ensure sufficient transparency on its beneficial owners or a company wholly-owned by such listed company.

6.3.5 Politically Exposed Persons: other measures

(1) The Company must take reasonable measures to determine:

(a) if a customer, or a Beneficial Owner of a customer, is a Politically Exposed Person (PEP);

(a) If a customer, or a Beneficial Owner of a customer, is a PEP, the Company must: obtain the approval of senior management to commence or continue the business relationship with the customer;

(b) take reasonable measures to establish the source of wealth and source of funds of the customer orBeneficial Owner; and

(c) increase the degree and nature of monitoring of the business relationship, to determine whether the customer's transactions or activities appear unusual or suspicious.

Sanctions and PEP screening is carried out for both legal entities and individuals using WebShieldvendor (https://www.webshield.com/); WebShield uses the MemberCheck database (https:// membercheck.com/), MemberCheck is a world-renowned provider of specialized databases.

6.4 Enhanced customer due diligence

6.4.1 Where the factors that may indicate higher money laundering risk described in 5.1.2 is discovered the Company is required to undertake Enhanced Customer Due Diligence. It must, to the extent applicable to the customer:

(a) obtain and verify additional:

(i) identification information on the customer and any Beneficial Owner;

(ii) information on the intended nature of the business relationship; and

(iii) information on the reasons for a transaction;

(b) update more regularly the Customer Due Diligence information which it holds on the customer and any Beneficial Owners;

(c) take reasonable measures to establish:

(i) the source of funds; and

(ii) the source of wealth,

of the customer or, if applicable, of the Beneficial Owner;

(d) increase the degree and nature of monitoring of the business relationship, in order to determinewhether the customer's transactions or activities appear unusual or suspicious;

and

(e) obtain the approval of senior management to commence a business relationship with a customer;

(f) where applicable, require that any first payment made by a customer in order to open an accountwith the Company must be carried out through a bank account in the customer's name with:

(i) a Bank;

(ii) a Regulated Financial Institution whose entire operations aresubject to regulation and

supervision, including AML regulation and supervision, in a jurisdiction with AML regulations which are equivalent to the standards set out in the FATF recommendations; or

(2) a Subsidiary of a Regulated Financial Institution referred to in (ii), if the law that applies to the Parent ensures that the Subsidiary also observes the same AML standards as its Parent.

6.5 Simplified customer due diligence

(1) Where the factors that may indicate lower money laundering risk described in 5.1.3 is discovered the Company may undertake Simplified Customer Due Diligence.

The Simplified Customer Due Diligence may include:

(a) verifying the identity of the customer and any Beneficial Owners after the establishment of the business relationship under Rule 7.2.1(3);

(b) deciding to reduce the frequency of, or as appropriate not undertake, customer identification updates;

(c) deciding not to verify an identification document other than by requesting a copy;

(d) reducing the degree of on-going monitoring of transactions, based on a reasonable monetary threshold or on the nature of the transaction; or

(e) not collecting specific information or carrying out specific measures to

understand the purpose and intended nature of the business relationship, but inferring such purpose and nature from the type of transactions or business relationship established.

6.6 Ongoing customer due diligence (Monitoring)

6.6.1 (1)When undertaking ongoing Customer Due Diligence the Company must, using the risk-based approach:

(a) monitor transactions undertaken during the course of its customer relationship to ensure that the transactions are consistent with the Company's knowledge of the customer and his business; Transaction Monitoring is performed by internally developed Risk Control System (RCS) , that covers 24/7 Sanction, PEP Screening as well as prevention of fraud scenarios and detection of suspicious transactions. RCS collects and analyzes such data as IP address, operation type, Customer ID etc.

(b) pay particular attention to any complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or legitimate purpose;

(c) enquire into the background and purpose of the transactions in (b);

(d) review the adequacy of the Customer Due Diligence information it holds on customers and Beneficial Owners to ensure that the information is kept up to date, particularly for customers with a high risk rating; and

(e) review each customer to ensure that the risk rating assigned to a customer remains appropriatefor the customer in light of the money laundering risks.

(2) The Company must carry out a regular monitoring periodically and at other appropriate times when a material change or event occurs relating to a customer such as when:

(a) the Company changes its CDD documentation requirements;

(b) an unusual transaction with the customer is expected to takeplace;

(c) there is a material change in the business relationship with the customer; or

(d) there is a material change in the nature or ownership of thecustomer.

6.6.2 Ongoing sanctions screening

The Company must review its customers, their business and transactions against United Nations Security Council Consolidated List, EU Terrorism List, Office of Foreign Assets Control (OFAC) Sanctions list,Interpolante List,Bureau of Industry And Security List,Department Of State Nonproliferation Sanctions List,HMT Financial Sanctions and against any other local and international sanctions lists and other sources provided on the International Monetary Fund, the World Bank, the FATF websites.

6.7 Failure to conduct or complete customer due diligence

(1) Where, in relation to any customer, the Company is unable to conduct or complete the requisiteCustomer Due Diligence in accordance with Rule 7.1.1 it must, to the extent relevant:

(a) not carry out a transaction with or for the customer through a bank account or in cash;

(b) not open an account or otherwise provide a service;

(c) not otherwise establish a business relationship or carry out a transaction;

(d) terminate or suspend any existing business relationship with the customer;

(e) consider whether the inability to conduct or complete Customer Due Diligence necessitates themaking of a Suspicious Activity Report.

(2) The Company is not obliged to comply with (1) if:

(a) to do so would breach of Federal AML legislation; or

(b) the FIU directs the Company to act otherwise.

7 RELIANCE AND OUTSOURCING

7.1 Reliance on a third party

7.1.1 (1) The Company may rely on the following third parties to conduct one or more elementsof Customer Due Diligence on its behalf:

(a) a law firm, notary, or other independent legal business, accounting firm, audit firm or insolvencypractitioner in U.A.E. or an equivalent person in another jurisdiction;

(b) a Financial Institution; or

(2) In (1), the Company may rely on the information previously obtained by a third party whichcovers one or more elements of Customer Due Diligence.

(3) Where the Company seeks to rely on a person in (1) it may only do so if and to the extent that:

(a) it immediately obtains the necessary Customer Due Diligence information from the third party in
(1);

(b) it takes adequate steps to satisfy itself that certified copies of the documents used to undertake the relevant elements of Customer Due Diligence will be available from the third party on request without delay;

(c) if the third party in (1) is in another country it has to be:

(i) subject to requirements in relation to customer due diligence and record keeping which meet the standards set out in the FATF Recommendations; and

(ii) supervised for compliance with those requirements in a manner that meets the standards for regulation and supervision set out in the FATF Recommendations;

(d) the third party (1) has not relied on any exception from the requirement to conduct any relevant elements of Customer Due Diligence which the Company seeks to rely on; and

(e) in relation to (2), the information is up to date.

(4) If the Company is not reasonably satisfied that a customer or Beneficial Owner has been identified and verified by a third party in a manner consistent with these Rules, the Company must immediately perform the Customer Due Diligence itself with respect to any deficiencies identified.

(5) Notwithstanding the Company's reliance on the third party in (1), the Company remains responsible for compliance with, and liable for any failure to meet the Customer Due Diligence requirements in this Programme.

7.1.2 (1) When assessing if requirements, supervision or regulation in another jurisdiction

meet FATF standards, the Company must take into account factors including, among other things:

(a) mutual evaluations, assessment reports or follow-up reports published by FATF, the IMF, the World Bank, the OECD or other International Organisations;

(b) membership of FATF or other international or regional groups such as the MENAFATF or the Gulf Co-operation Council;

(c) contextual factors such as political stability or the level of corruption in the jurisdiction;

(d) evidence of recent criticism of the jurisdiction, including in:
(i) FATF advisory notices;

(ii) public assessments of the jurisdiction's AML regime by organisations referred to in (a); or

(iii) reports by other relevant non-government organisations or specialist commercial organisations;
and

(2) The Company making an assessment under (1) must rely only on sources of information thatare reliable and up-to-date

(3) The Company must keep adequate records of how

it made its assessment,including the sources and materials

considered.

7.2 Outsourcing

7.2.1 A Company which outsources any one or more elements of its Customer Due Diligence to the third party (service provider) remains responsible for compliance with, and liable for any failure to meet, suchobligations.

8 SANCTIONS AND OTHER INTERNATIONAL OBLIGATIONS

8.1 Relevant United Nations resolutions and sanctions

8.1.1 (1) The Company must establish and maintain effective systems and controls to ensure that on an ongoing basis it is properly informed as to, and takes reasonable measures to comply with, relevant resolutions or sanctions issued by the United Nations Security Council.

The Company implements appropriate screening procedures to ensure that customers, its employees and transactions are not identified on any local and international financial sanctions lists which include but are not limited to: United Nations Security Council Consolidated List, EU Terrorism List, Office of Foreign Assets Control (OFAC) Sanctions list, Interpolante List, Bureau of Industry And Security List, Department Of State Nonproliferation Sanctions List, HMT Financial Sanctions and against any other local and international sanctions lists and other sources provided on the International Monetary Fund, the World Bank, the FATF websites.

For this purposes the Company may rely on a third parties or conduct sanction screening manually.

(2) The Company must immediately notify the DMCCA and FIU when it becomes aware that it is:

(a) carrying on or about to carry on an activity;

(b) holding or about to hold money or other assets; or

(c) undertaking or about to undertake any other business whether or not arising from or inconnection with (a) or (b);

for or on behalf of a person, where such carrying on, holding or undertaking constitutes or may constitute a contravention of a relevant sanction or resolution issued by the United Nations Security Council.

8.2 Government, regulatory and international findings

8.2.1 (1) The Company established and maintained systems and controls to ensure that on an ongoing basis it is properly informed as to, and takes reasonable measures to comply with, any findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions issued by:

(a) the government of the U.A.E. or any government departments in the U.A.E.;

(b) the Central Bank of the U.A.E. or the FIU;

(c) FATF;

(d) U.A.E. enforcement agencies; and concerning the matters in

(2) For the purposes of (1), the relevant matters are:

(a) arrangements for preventing money laundering, terrorist financing or the financing of weapons of mass destruction in a particular country or jurisdiction, including any assessment of material deficiency against relevant countries in adopting international standards; and

(b) the names of persons, groups, organisations or entities or any other body where suspicion of money laundering or terrorist financing or the financing of weapons of mass destruction exists.

(3) For the purposes of (1), measures in a finding that the Company must comply with include, butare not limited to, measures:

(a) requiring specific elements of enhanced due diligence;

(b) requiring enhanced reporting mechanisms or systematic reporting of financial transactions;

(c) limiting business relationships or financial transactions with specified persons or persons in a specified jurisdiction;

(d) prohibiting the Company from relying on third parties located in a specified jurisdiction to conduct customer due diligence;

(e) requiring correspondent relationships with banks in a specified jurisdiction to be reviewed, amended or, if necessary, terminated;

(f) prohibiting the execution of specified electronic fund transfers; or

(g) requiring increased external audit requirements for financial groups with respect to branches and subsidiaries located in a specified jurisdiction.

9 MONEY LAUNDERING REPORTING OFFICER

9.1 Appointment of a MLRO

9.1.1 (1) The Company must appoint an individual as MLRO, with responsibility for implementation and oversight of its compliance with the Rules in this Programme, who has an appropriate level of seniority and independence to act in this role.

9.1.2 The Company's MLRO must deal with the DMCCA in an open and co-operative manner and must disclose appropriately any information of which the DMCCA would reasonably be expected to be notified.

9.1.3 The Company may outsource the role of MLRO to an individual outside the Company provided that the relevant individual under the outsourcing agreement is and remains suitable to perform theMLRO role.

9.2 Qualities of a MLRO

9.2.1 The Company ensures that its MLRO has:

(a) direct access to its senior management;

(b) sufficient resources including, if necessary, an appropriate number of appropriately trained employees to assist in the performance of his duties in an effective, objective and independent manner;

(c) a level of seniority and independence within the Company to enable him to act on his ownauthority; and

(d) timely and unrestricted access to information sufficient to enable him to carry out his responsibilities.

9.3 Responsibilities of a MLRO

9.3.1 The Company must ensure that its MLRO implements and has oversight of and is responsible for the following matters:

(a) the day-to-day operations for compliance by the Company with its AML procedures, systemsand controls;

(b) acting as the point of contact to receive notifications from the Company's employees;

(c) taking appropriate action following the receipt of a notification from an employee ;

(d) making Suspicious Activity Reports in accordance with Federal AML legislation;

(e) acting as the point of contact within the Company for competent U.A.E. authorities and the DMCCA regarding money laundering issues;

(f) responding promptly to any request for information made by competent the U.A.E. authorities or the DMCCA;

(g) establishing and maintaining an appropriate money laundering training programme and adequateawareness arrangements:

(h) investigating transactions related to alleged crimes;

(i) producing reports to senior management concerning adherence to compliance policies, procedures.

(j) notifying DMCCA promptly regarding any communication from other State authorities concerningAML matters.

10 AML TRAINING AND AWARENESS

10.1Training and awareness

10.1.1 The Company must

(a) provide annual AML training to all employees;

(b) ensure that its AML training enables its employees to:

(i) understand the relevant legislation relating to money laundering, including Federal AML legislation;

(ii) understand its policies, procedures, systems and controls related to money laundering and anychanges to these;

(iii) recognise and deal with transactions and other activities which may be related to moneylaundering;

(iv) understand the types of activity that may constitute suspicious activity in the context of the business in which an employee is engaged and that may warrant a notification to the MLRO;

(v) understand its arrangements regarding the making of a notification to the MLRO;

(vi) be aware of the prevailing techniques, methods and trends in money laundering relevant to the business of the Company;

(vii) understand the roles and responsibilities of employees in combating money laundering,including the identity and responsibility of the Company's MLRO and deputy, where applicable; and

(viii) understand the relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions; and

(c) ensure that its AML training:

(i) is appropriately tailored to the Company's activities, including its products, services, customers, distribution channels, business partners, level and complexity of its transactions; and

(ii) indicates the different levels of money laundering risk and vulnerabilities associated with the matters in (c)(i).

11 SUSPICIOUS ACTIVITY REPORTS

11.1Application and definitions

11.1.1 In this chapter, "money laundering" and "terrorist financing" mean the criminal offencesdefined in the Federal AML legislation.

11.1.2 The following examples of situations might give rise to suspicion in certain circumstances:

- transactions or instructions which have no apparent legitimate purpose and/or appear not to have a commercial rationale;

- transactions, instructions or activity that involve apparently unnecessary complexity or which do not constitute the most logical, convenient or secure way to do business;

- where the transaction being requested by the customer, without reasonable explanation, is out of the ordinary range of services normally requested, or is outside the experience of the financial services business in relation to the particular customer;

- where occasional transactions are carried in favor of a customer for amounts equal to or exceeding AED 55,000 (approximately $15,000), whether the transaction is carried out in a single transaction or in several transactions that appear to be linked; or where occasional transactions are carried out in the form of wire transfers for amounts equal to or exceeding AED 3,500 (approximately $950);

- where, without reasonable explanation, the size or pattern of transactions is out of line with any pattern that has previously emerged; where the customer refuses to provide the information requested without reasonable explanation or who otherwise refuses to cooperate with the CDD and/or ongoing monitoring process;

- where a customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period without a reasonable explanation;

- the extensive use of trusts or offshore structures in circumstances where the customer's needs are inconsistent with the use of such services;

- transfers to and from high risk jurisdictions without reasonable explanation, which are not consistent with the customer's declared business dealings or interests;

- unnecessary routing of funds or other property from/to third parties or through third party accounts.

11.2Internal reporting requirements

11.2.1 The Company controls to ensure that whenever any employee, acting in the ordinary course of his employment, either:

(a) knows;

(b) suspects; or

(c) has reasonable grounds for suspecting;

that a customer is engaged in or attempting money laundering or terrorist financing or suspicious activity described in 11.1 , that employee promptly notifies the Company's MLRO and provides the MLRO with all relevant details.

11.3Suspicious activity report

11.3.1 The Company must ensure that where the Company's MLRO receives an suspicious activityreport under 11.2. , the MLRO, without delay:

(a) inquiries into and documents the circumstances in relation to which the notification made under Rule 11.2.;

(b) determines whether in accordance with Federal AML legislation a Suspicious Activity Report must be made to the FIU and documents such determination;

(c) if required, makes a Suspicious Activity Report to the FIU as soon as practicable; and

(d) notifies the DMCCA of the making of such Suspicious Activity Report immediately following its submission to the FIU.

11.4 Notifications

Where the Company receives a request for information or inspection from any State authority regarding enquiriesinto potential Money Laundering, Terrorist Financing activity carried on, it should respond promptly.

11.5 Record keeping

11.5.1 The Company must maintain the following records:

(a) a copy of all documents and information obtained in undertaking initial and ongoing CustomerDue Diligence;

(b) records (consisting of the original documents or certified copies) in respect of the customerbusiness 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, such as if the transaction or business is unusual or suspicious, whether or not it results in a Suspicious Activity Report;

(c) notifications made under 11.2;

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

(e) any relevant communications with the FIU;

(f) any other matter that the Company is expressly required to record under the Programme,

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

11.5.1 The Company must provide to the DMCCA or a law enforcement agency immediately onrequest a copy of a record referred to in 11.5.1.

11.5.2 Where the records referred to in 11.5.1 are kept by the Company outside the DMCC, theCompany must:

(a) take reasonable steps to ensure that the records are held in a manner consistent with theseProgramme;

(b) ensure that the records are easily accessible to the Company; and upon request by the DMCCA,ensure that the records are immediately available for inspection.

APPENDIX 1: Prohibited Products and Services

The company reserves the right to expand this list by introducing types of business that may be associated with the distribution of weapons, drugs, prohibited content, financing of terrorism, inciting racial and religious war, violation of human rights or other local and international laws.

The company can also refuse a client whose type of business may be considered high risk during KYC checks.

Business &Services	Description of Prohibited Activity Types
Adult Content	Any merchant connected with visual content, such as pornography or violence that is not generally thought to be appropriate for viewingby children.
Alcohol sales via Internet	Merchants selling alcohol products via internet, even if the sale of those items is not restricted to the merchant own country of domicile.
Chemicals and Allied Products — not elsewhereclassified	Wholesale distributors of chemicals and allied products not elsewhere classified. Products for sale are typically used for industrial purposes. Examples include industrial acids, ammonia andalcohol, heavy, aromatic and other chemicals, chlorine, compressed and liquefied gases, detergents, fuel and oil additives, resins, salts, turpentine, sealants, rust proofing chemicals, coal tar products, dry ice, dyestuffs, glue,gelatin, and explosives.
Child Pornography	Any merchant who provides products or servicesassociated with actual or suggested child pornography. Includes any merchant or website who uses the following terminology to promote their product: "lolita," "pedo," "pre-teen," or any other terminology that suggests childpornography.
Cigarette/electronic cigarette/Tobacco/ Vape	Merchants that sell cigarettes/electronic cigarette/tobacco/vape via Internet even if thesale of those items is NOT

Sales	restricted to the merchants own country of domicile.
Counterfeit goods	Merchants selling counterfeit merchandise (well-known brands) or goods where merchantsare infringing on intellectual property rights of trade mark owners (including illegal use ofgames, game keys e.t.c.)
Dealers of high-value precious goods and ect.	Businesses involved in the sale of goods of highvalue. Examples of these businesses include antique dealers, boat and car sales, dealers in precious stones, jewellers.
Drug Paraphernalia	Any business whose products are solely intended for aiding the consumption of illegaldrugs.
Financial and other Pyramid Sales	Includes sales structures where multiple levels of sales people are making money off one another with no real product or a questionable product to sell: income of the first participants of pyramid is paid at the expense of newparticipants.
Fortune tellers	Includes fortune-tellers, tarot card readers, andmystics.
Guns, firearms, munitions sale &distribution	Any sale of firearms by any method including production/recycling of explosive and nuclearfuel.
Non-prescription drugs such as pharmaceutical wonder drugs e.g. Steroids, diet pills & all Internet drug stores.	Outlets offering nonprescription drugs such as: pharmaceutical wonder drugs e.g. steroids, dietspills, and all Internet drug stores.
Political Organizations and parties	Merchants representing the membership organizations that promote the interests of a national, state, or local political party or candidate, including political groups organized specifically to raise funds for a political party orindividual candidate.

Religious Organizations (excludingnationally recognized religious organizations/faiths)	Religious organizations that provide worshipservices, religious training or study, and religious activities, including collection of donations.
Sexual Encounter/Escort Firms	Any merchant connected with sexual encounter, including escort services, massage parlors, spas,etc., where sexual encounters are permitted.