Bullion Link Trading - FZCO

Policy for Anti-Money Laundering & Counter Financing of Terrorism

Version Control

	Who
Owner Entity	Bullion Link Trading - FZCO
Domain	Compliance & Governance
Topic	AML/CFT Policy
Policy Owner	
Effective Date	05 February 2025
Revision Date	06 February 2026
Version	V1

Contents

1. INTRODUCTION

(1) Money Laundering is the process by which criminals attempt to hide or disguise the true origin and ownership of the proceeds of their criminal activities. If carried out successfully, money laundering enables criminals to escape prosecution, maintain control over the proceeds of crime and continue their criminal activities. Money laundering also includes terrorist financing.

(2) Involvement in money laundering, whether knowingly or unknowingly, may result in criminal liability and severe reputational damage to Bullion Link Trading - FZCO ("The Company").

(3) The Company therefore places the utmost importance on complying with all applicable laws and regulations for the prevention of money laundering and shall use the policies and procedures set out in this Policy to prevent its business from being used for illicit activities.

1.1. About this Policy

(1) This Anti-Money Laundering Policy ("Policy") applies to all Employees, which term, for the purposes of this Policy, including but not limited to the members of the Board of Directors, all senior managers, operational staff and any Employee with Customer contact or who handles Customer transactions.

(2) This Policy is prepared to provide Employees with a good understanding of what they and The Company, shall do to comply with the laws and regulations for the prevention of money laundering and terrorism financing in the UAE and how to recognise and report that such activity may be taking place.

(3) For any clarification regarding this Policy, employees should consult with the Compliance Officer ("CO"). The contact details are as follows:

Role	Name	Email	Mobile
CO			

(4) Capitalised terms are defined in the Glossary set out at Appendix A to this Policy. Any reference to "money laundering" in lower case includes a reference to terrorist financing unless the context indicates otherwise.

1.2. Applicable laws and regulations

The main laws and regulations applicable in the UAE to The Company and its Employees are:

- Federal Decree – Law No (20) of 2018 on Anti –Money Laundering and Combating the Financing of terrorism and financing of illegal organizations
- Cabinet Decision No (10) of 2019 concerning the Implementing regulation of Decree Law No (20) of 2018 on Anti Money Laundering and Combatting the Financing of Terrorism and Financing of Illegal Organisations
- UAE Cabinet Decision No. 74 of 2020 regarding Terrorism Lists Regulation and Implementation of UNSC Resolutions
- Cabinet Decision No. 16 of 2021 regarding the unified list of the violations and administrative fines
- Federal Decree Law No (26) of 2021 Amending Certain Provisions of Federal Decree Law No. (20) for 2018 on Anti-Money Laundering and Combatting the Financing of Terrorism and Financing of Illegal Organisations
- Circular No. 08/AML/2021 to Dealers in Precious Stones and Metals licensed in the United Arab Emirates
- Cabinet Resolution No. (24) of 2022 on Combatting Money Laundering and the Financing of Terrorism and Illegal Organisations
- Cabinet Decision 109 of 2023 regulating the Beneficial Owner Procedures
- Cabinet Decision 132 of 2023 regarding the Administrative Penalties

1.3. Offences and penalties

(1) Money laundering: Under Article 2 of the Combating Money Laundering and Terrorism Financing Crimes law, whoever commits any of the following acts, despite being fully aware that such funds are derived from an offence or a misdemeanour, shall be deemed a perpetrator of money laundering if it:

(a) converts, transfers, deposits, saves, invests, exchanges or manages any proceeds, with intent to conceal or disguise the illicit origin thereof.

(b) conceals or disguises the true nature, origin, location, way of disposition, movement, rights related to any proceeds or ownership thereof.

(c) acquires, possesses or uses such proceeds.

(2) **Failing to report:** Under Article 15 of the Combating Money Laundering and Terrorism Financing Crimes law, the chairman, directors, managers and employees of the Financial Institutions or Other Financial, Commercial and Economic Establishments who are aware of any offence, occurring within their establishments relating to money laundering, terrorism and terrorist organizations financing, yet refrain from notifying the Financial Intelligence Unit, are subject to be punished by law.

(3) **Tipping off:** Under Article 16 of the Combating Money Laundering and Terrorism Financing Crimes law, whoever informs any person of any proceedings under scrutiny relating to possible involvement in suspicious transactions, or that the competent authorities are investigating the same, are subject to be punished by law.

(4) The Company or any of its Employees may be liable for the offence of money laundering if such an activity is intentionally committed in its name or for its account and The Company and any of its Employees may face the Authority enforcement action in respect of any breach of any Rule in the AML Module. Employees are specifically advised that they may face penalties if they fail to report suspicions of money laundering or if they "tip off" a person that is under investigation.

(5) The potential penalties for individuals and/or institutions regarding money laundering offences may comprise fines and/or imprisonment.

1.4. Summary obligations

(1) Employees must comply with the matters set out in this Policy including their obligation to participate in Anti-Money laundering awareness training.

(2) Employees shall:

(a) report to the CO/MLRO without delay if they know, suspect or have reasonable grounds for knowing or suspecting that a Person may be engaged in money laundering; and

(b) not alert that person to their suspicion or the fact that they have made a report.

2. KEY ELEMENTS OF THE COMPANY'S AML PROGRAM

The key elements of The Company's policies, procedures, systems and controls for the prevention of money laundering include but are not limited to the following:

2.1. Risk-based approach

- Identifying money laundering risks and those presented by each Customer and taking a considered, risk-based, approach to eliminate, mitigate or manage them.

- Undertaking the appropriate amount of Customer due diligence on its customers having regard to the risks that have been identified in each case rather than by taking a routine, tick-the-box approach.

- Ensuring that higher risk business relationships, including relationships involving Politically Exposed Persons (PEPs), their associates or close family members, are accepted only with the Board of Directors' explicit approval and understanding of the potential higher risks involved.

2.2. Staff awareness and training

- Ensuring staff are aware of the money laundering risks, their obligations and liabilities under applicable laws and regulations, The Company's procedures for undertaking Customer due diligence and how to recognise and report suspicious activity.

2.3. Customer due diligence[1]

- Verifying Customers identity (and their Beneficial Owners, where relevant) and understanding their source of funds/wealth.

- Taking into account Global, Regional and Local guidelines, regulations and sanctions lists and checking that the Company's Customers, Partners and Suppliers are not subject to any of the jurisdiction's lists.

2.4. Prohibited business

- Carrying on business with persons whose ultimate Beneficial Owners cannot be identified or with nominees acting on behalf of persons whose identity has not been disclosed.

[1] Refer to KYC Policy

- Allowing a business relationship to commence before the Customer due diligence has been completed.

2.5. On-going due diligence and Customer activity monitoring

- Key information about customers up to date and verifying any significant changes.

- Monitoring the Customer's activities and Transactions throughout the lifecycle of the relationship.

2.6. Reporting of knowledge or suspicion of money laundering

- Internally, by the Employee to the CO/MLRO.
- Externally, by the CO/MLRO to the Financial Intelligence Unit

3. SENIOR MANAGEMENT ARRANGEMENTS & RESPONSIBILITIES

3.1. Board of Directors

(1) Ultimate responsibility for compliance with the policies, procedures, systems and controls set out in this Policy rests with the Board of Directors.

(2) Specifically, the Directors are responsible for:

(a) establishing and maintaining effective policies, procedures, systems and controls to prevent opportunities for money laundering in relation to The Company and its activities;

(b) ensuring that the AML systems and controls:

(i) include the provision to the Board of regular management information on the operation and effectiveness of its AML systems and controls necessary to identify, measure, manage and control money laundering risks;

(ii) enable it to determine whether a Customer or a Beneficial Owner is a Politically Exposed Person;

(iii) enable The Company to comply with all applicable laws and regulations; and

(c) ensuring that regular risk assessments are carried out on the adequacy of the 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 the business activity.

(3) All Employees are responsible for their day-to-day compliance with these policies and procedures.

3.2. The Compliance Officer / Money Laundering Reporting Officer

(1) The Compliance Officer ("CO") or Money Laundering Reporting Officer ("MLRO") is responsible for the implementation and oversight of The Company's compliance with the UAE Authorities.

(2) The CO/MLRO shall work in an open and cooperative manner with the Authorities.

(3) The CO/MLRO shall have timely and unrestricted access to all necessary information to perform his/her duties in an effective, objective and independent manner.

(4) All Employees are required to cooperate fully with the CO/MLRO in the performance of his/her duties.

3.3. Responsibilities of the CO/MLRO

(1) The CO/MLRO is responsible for the implementation and oversight of the following:

(a) the day-to-day operations in compliance with the AML policies, procedures, systems and controls, including signing off on all new client acceptance decisions;

(b) acting as the point of contact to receive internal SARs from Employees;

(c) taking appropriate action to (i) investigate and document the circumstances in which the internal SAR was made; (ii) determine and document whether an external SAR shall be filled to the UAE Financial Intelligence Unit ("FIU");

(d) if required, filling an external SAR to the FIU as soon as practicable and notifying the designated Authority immediately following its submission to the FIU that such report has been made;

(e) acting as the point of contact with the competent U.A.E. authorities regarding money laundering issues;

(f) recommending, designing and implementing a mitigation plan

(g) responding promptly to any request for information made by competent U.A.E. authorities

(h) receiving and acting upon any relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions issued by (i) the UAE government, or any government department in the U.A.E., (ii) the Central Bank of the UAE or the FIU, (iii) the Financial Action Task Force, (iv) U.A.E. enforcement agencies, (v) the Ministry of Economy; (vi) Executive Office for Control and Non-Proliferation; or (vii) the United Nations Security Council concerning (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 or (b) the names of persons, groups, organisations or entities or any other body where suspicion of money laundering or terrorist financing or financing of weapons of mass destruction exists;

(i) establishing and maintaining an appropriate money laundering training programme and adequate awareness arrangements, as set out in Section 8 of this Policy.

(2) The Company and the CO/MLRO shall co-operate openly with the Authorities and disclose appropriately any information of which the Authorities would reasonably be expected to be notified.

3.4. Internal audit

(1) The Company shall commission regular reviews and assessments of the effectiveness of its money laundering policies, procedures, systems and controls, and its compliance with them. Such reviews shall specifically cover the following:

(a) sample testing of compliance with The Company's CDD arrangements;

(b) an analysis of all notifications made to the CO/MLRO to highlight any area where procedures or training may need to be enhanced; and

(2) Such reviews shall be carried out by the Internal Audit function at least annually.

3.5. Notification to UAE Authorities

(1) The Company shall notify the Authorities in writing as soon as possible if it:

(a) receives a request for information from a regulator or agency responsible for AML or counter-terrorism financing regarding enquiries into potential money laundering or terrorist financing;

(b) becomes aware, or has reasonable grounds to believe, that a money laundering event has occurred or may have occurred in or through its business;

(c) becomes aware of any money laundering or sanctions matter in relation to The Company or a member of its Group which could result in adverse reputational consequences to The Company; or

(d) becomes aware of any significant breach of a Rule in the AML module or breach of Federal Law No. 4 of 2002 or Federal Law No.1 of 2004 by The Company or any of its Employees.

4. THE RISK-BASED APPROACH

4.1. Overview

(1) The Company adopts a risk-based approach that is proportionate to the money laundering risks presented by the nature of its business, Customers, products and services.

(2) The Company's risk-based approach involves:

(a) business risk assessments: periodic assessments of The Company's business which enable the Board of Directors to understand the money laundering risks facing The Company, assess The Company's vulnerabilities to those risks and take all reasonable steps to eliminate or manage the risks;

(b) Customer risk assessments: assessments of the money laundering risks presented by each Customer of The Company; and

(c) risk mitigation by means of Customer due diligence and on-going monitoring that is proportionate to the risks that have been assessed.

(3) These risk-based assessments are coordinated and overseen by the CO/MLRO who ensures that they are (i) properly documented and (ii) reviewed, and if necessary updated, at least annually.

4.2. Business risk assessment

(1) The Company's business risk assessment identifies and takes account of any vulnerabilities relating to:

(a) its type of Customers and their activities;

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

(c) its products, services and activity profiles;

(d) its distribution channels and business partners;

(e) the complexity and volume of its business;

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

(g) the use of new or developing technologies for both new and pre-existing products.

(2) The Company uses the information obtained in its business risk assessments to develop and maintain its AML policies, procedures, systems and controls to ensure that they adequately mitigate the risks that have been identified, assess their effectiveness, assist in the allocation and prioritization of AML resources and in carrying out its customer risk assessments.

4.3. Customer risk assessment

(1) The Company shall undertake a customer risk assessment of all its customers. The customer risk assessment shall be documented on a Customer Risk Assessment Form (See Appendix A to the Business AML Risk Assessment). Customer Risk Assessment shall include but not limited to:

(a) Potential high-risk Customers

(b) Politically exposed persons

(c) Prohibited Customer

5. CUSTOMER DUE DILIGENCE

(1) Customer Due Diligence is the process that The Company uses to gather information about its Partners. This process involves several steps including but not limited to:

(a) Identification and verification of Natural Persons

(b) Identification of Legal Persons

(c) Identification and verification of Beneficial Owners

(d) Transaction Monitoring

6. REPORTING OBLIGATIONS

6.1. Overview

Transaction reporting is a fundamental regulatory obligation that The Company rigorously adheres to within the United Arab Emirates (UAE). This process encompasses the systematic identification, analysis, and reporting of financial transactions, serving several key aims. Primarily, transaction reporting aims to detect and prevent money laundering, terrorism financing, and other illicit activities within the financial system. Additionally, it facilitates regulatory compliance, ensuring adherence to UAE's stringent Anti-Money laundering (AML) and counter-terrorism financing (CTF) regulations. Furthermore, transaction reporting fosters transparency and accountability, bolstering trust in the integrity of the financial sector. Through meticulous transaction reporting practices, The Company demonstrates its unwavering commitment to regulatory compliance, financial integrity, and combating financial crime within the UAE.

6.2. Dealers in Precious Metals and Stones Reporting (DPMSRs)

(1) The Company shall report all qualifying transactions above AED 55,000 received from customers on the GoAML platform.

(2) All transactions meeting the following conditions shall be reported:
   (a) Cash transactions with UAE residents and non-resident individuals equal to or exceeding AED55,000
   (b) Cash transactions with legal entities equal to or exceeding AED55,000.
   (c) International wire transfers from legal entities equal to or exceeding AED55,000.
   (d) Instalment transactions received in cash, exceeding the threshold OF AED55,000;
   (e) Advance payments in cash exceeding AED55,000

(3) All qualifying transactions are to be reported within 2 weeks of receipt.

6.3. Reporting and filling of STR's/SAR's:

(1) This Policy mandates the investigation of all alerts that may be suspicious and documents the steps taken in the investigation in the form of an Internal Suspicious Transaction Report ("ISTR").

(2) The CO/MLRO determines whether a Suspicious Transaction Report ("STR") is necessary based on the findings. Once decision has been made to proceed with an STR, the CO/MLRO is responsible to

raise an STR to the FIU of the Central bank of UAE to notify the activity /transaction through the GoAML platform.

(3) An STR shall be filled:

a. If further investigation is required and the suspect is unknown, an STR shall be filed on detection of the suspicious activity.

b. Even if the transaction is not reported, the CO/MLRO shall set forth the findings in writing and the same shall be retained.

c. The Compliance Department shall maintain a register for recording the Suspicious Transaction Reports made to or by the Compliance Officer/MLRO. The same shall be retained for a period of five years with the records of any actions taken.

d. By ignoring key indicators on Money laundering/ Terrorist Financing, an employee is considered to have directly partaken in such an activity through “willful blindness”. (Willful Blindness is when an employee becomes suspicious about a customer/transaction but does not report the suspicion even though the employee is aware that the transaction is of an illegal nature or that the intentions of the customer’s transaction is money laundering/terrorist financing.)

e. In case a suspicious activity is identified the CO/MLRO may decide to seek appropriate permissions from the Central Bank of the UAE to freeze such funds. In case the Central Bank approves the request to freeze the funds, the same should be for a period not exceeding 7 working days. Upon freezing the funds, the customer should be notified of the decision with instructions to provide the relevant documentation to ascertain the soundness of the transaction.

f. All relevant details of any internal and external STR shall be kept in safe custody of the Compliance Department.

7. RED FLAG INDICATORS

7.1. Overview

(1) The red flag indicators that follow are meant to help DPMSs to identify some of the circumstances that could be suspicious in nature. They could indicate that property may represent proceeds of money laundering ("ML") or terrorism financing ("TF") or used/intended to be used in connection with ML or TF.

(2) While each individual indicator may not be sufficient by itself to suggest ML or TF, a combination of the indicators may indicate a suspicious transaction.

(3) The list is not exhaustive. It may be updated due to changing circumstances and new methods of laundering money or financing terrorism. Please refer to the UAE Central Bank's website for the latest list of red flags.

7.2. Transaction Patterns of Customers

(1) Transactions that are not consistent with the usual profile of a customer:

a. Transactions that appear to be beyond the means of the customer based on his/herstated or known occupation or income;

b. Transactions that appear to be more than the usual amount or quantity for a typical customer of the business; or

c. Transaction purposes that are not in line with the known or expected operations ofthe business.

(2) Large amounts of cash, traveller's cheques, cashier's cheques or trade-ins involved in the transactions.

(3) Large or frequent transactions that are made in a foreign currency.

(4) Transactions in which third parties are involved, either as payers or recipients of payment, without apparent legitimate business purpose. For example:

a. Payments received from a third party, who is not the owner of the funds, without legitimate business purpose.

b. Payments of proceeds made to third parties overseas, although the transaction is

between a domestic buyer and seller, and without apparent legitimate business purpose.

c. Precious Stones and Precious Metals delivered to a third party, who is not the owner or payer of funds, withoutlegitimate business purpose; or

d. Refunds paid to a third party, who is not the owner or payer of funds, without legitimate business purpose.

(5) Transactions with no apparent business purpose among associates or trading accounts forother Dealers and asset-backed tokens traded using bullion, investment or asset-backed token.

(6) Large transactions which are cancelled shortly after deposits or full payment are made, resulting in refunds. For example, the customer may pay for the transaction in cash andrequest the refund be issued in the form of a cheque. Conversely, the transaction may be made with a credit card and the customer request for the refund to be in cash or other means.

(7) Overpayment of transactions with a request to refund excess in cash or to a third party.

(8) Transactions involving virtual assets, especially where ownership of the virtual assets cannotbe easily traced to the customer.

(9) Transactions involving the use of stolen or fraudulent payment instruments, for example a payment card that appears stolen or altered or not issued in the customer's name. Some other possible indicators of suspicious online payment 'card-not-present' transactions could include:

a. Same shipping address, but different payment cards: Multiple online orders with mismatched payment card information could signify a criminal attempting to use aseries of stolen or fraudulent payment cards with the cards are still active.

b. Same payment account, but different shipping addresses: Multiple online orders with mismatched payment card information could signify a criminal attempting touse a series of stolen or fraudulent payment cards while the cards are still active.

c. Same Internet Protocol address (IP address): Online orders made from the same IPaddress, especially at or around the same time, but with different payment cards could signify criminals attempting to use fraudulent payment cards.

d. Reattempting with smaller transaction amount: When an online order is flagged as a potential fraud and declined, criminals may attempt to quickly purchase another item that costs less.

7.3. Customer Behaviour

(1) The customer appears to be structuring amounts to avoid customer identification or reporting threshold. For example, numerous transactions by a customer, especially over a short period of time, such that the amount of each transaction is not substantial (e.g., belowthe regulatory threshold for CDD), but the cumulative total of which is substantial.

(2) The customer makes enquiries about refund policies and requests for large refunds subsequently.

(3) The customer is suspected of using forged, fraudulent, or false identity documents fordue diligence and record keeping purposes, e.g., the customer presents identification documents with recent issue dates.

(4) The customer is unusually concerned with the Company's AMLCFT Policy.

(5) The customer fails to provide sufficient explanation and/or documents for the source of funds for his transaction. For example, the customer attempts to use a third-party cheque orcredit card in which the source of funds or underlying ownership cannot be easily traced to the customer or is questionable.

(6) The customer attempts to maintain a high degree of secrecy with respect to the transaction,for example:

a. To request that normal business records not to be kept; or
b. The customer is unable or unwilling to provide information for due diligence and record keeping purposes.
c. The customer is unable or unwilling to identify beneficial owners or controlling interest, where this would be commercially expected.
d. The customer is vague or refuses to provide information on the reason for buying or selling the metals, or about the origin of the items.

(7) The customer or the declared owner of the funds is traced to negative news or crime. For

example, the person is named in a reliable source (which can include a media or other open sources) that the person is suspected of being involved in illegal activity or detected when screened against UN Security Council Resolutions (UNSCRs).

(8) The customer appears to be related to a high-risk country or territory or entity that is associated with money laundering or terrorism activities or a person that has been designated as terrorists.

(9) The customer dramatically increases purchases of Precious Metals for no apparent reason or is willing to sell Precious Metals at a rate significantly lower than their typical sale value.

(10) The customer is employed by a DPMS but is dealing in his personal capacity.

(11) The customer uses alternative addresses for delivery such as a General Post Office (GPO), private service provider mailbox or third parties to receive purchases.

(12) The customer appears to be in a hurry to complete the transaction.

(13) The customer purchases Precious Metals without consideration for the value, size and/or colour of the Precious Metals or other costs (e.g., the extra expense of rush shipping) in the transaction.

(14) The customer is accompanied by others who appear suspicious (e.g., lurking outside the premises and closely monitoring the customer) and is in doubt when asked for further details.

(15) The customer requests to alter the transaction after being asked for identity documents.

(16) The customer makes unnecessary self-disclosure that his funds are clean and not involved in any money-laundering activities.

(17) The customer pays excessively for an item beyond its expected selling price in an auction.

(18) The customer insists on using cash to pay for excessively high value transactions when there is no apparent economic reason.

7.4. Transaction Pattern of Suppliers

(1) Transactions that are not consistent with the usual profile of a supplier:

a. Over or under-invoicing, structured, complex, or multiple invoice requests, and high-dollar shipments that are over or underinsured; or
b. Transactions which are excessive, given the amount or quality, or potential profitfrom the sale; or
c. Consignment size or type of product shipped appears inconsistent with the capacity ofthe exporter or importer. For example, the shipment or trans-shipment that does not make economic sense.
d. Misclassification of gold purity, weight, origin and value on customs declarationforms.

e. The transaction involves the use of front or shell companies, which have no real operating activity. For example, the entity's ownership structure appears to be doubtful or obscure or the entity refuses to provide additional information when requested.

(2) Transactions in which third parties are involved, either as payers or recipients of payment or Precious Metals, without apparent legitimate purpose.
a. Funds paid to a third party who is not related to the supplier, without legitimatebusiness purpose; or
b. Precious Metals delivered from a third party who is not related to the supplier, without legitimate business purpose.

(3) Transaction involving virtual assets, especially where ownership of the virtual assets cannotbe easily traced to the regulated dealer and supplier.

7.5. Supplier Behaviour

(1) The supplier is unable to provide information for due diligence and record-keeping purposes.

(2) The supplier is suspected of using forged, fraudulent, or false identity documents for duediligence and record keeping purposes.

(3) The supplier's origins of Precious Metals appear to be fictitious, doubtful or cannot be explained. For example, the supplier sells a large amount of Precious Metals that originate or are known to be traded from areas not known for their production i.e. trading centers.

(4) The supplier is unusually concerned with the Company's s AML/CFT policies.

(5) The supplier attempts to maintain a high degree of secrecy with respect to the transaction,for

example:

a. Request that normal business records not to be kept; or
b. Unwillingness to identify beneficial owners or controlling interests, where this would be commercially expected; or
c. Request for payments to be made through money services businesses or other non-bank financial institutions for no apparent legitimate business purposes

(6) Is vague or refuses to provide information on the reason for selling or buying Precious Metals, or about the origin of the items.

(7) (For diamonds only) Rough diamonds are not accompanied by a valid Kimberley Process (KP) certificate. For example:

a. No KP certificate attached to the shipment of rough diamonds; or
b. The KP certificate is or appears to be forged; or
c. The KP certificate has a long validity period.

(8) The supplier is traced to negative news or crime. For example, the person is named in areliable source (which can include a media or other open sources) that the person is suspected of being involved in illegal activity, or detected when screened against UNSecurity Council Resolutions (UNSCRs).

(9) The supplier appears to be related to a high-risk country or territory or entity that is associated with risk for money laundering or terrorism activities or a person that has beendesignated as terrorists.

(10) The supplier transports the Precious Metals through a country or territory that is designated as 'highrisk for money laundering or terrorism activities' for no apparent economic reason.

(11) The location to which the Precious Metals are moved directly to or from storage, is different from thesupplier's listed address.

(12) The supplier uses alternative addresses as a General Post Office (GPO), private serviceprovider mailbox which appears to be concealing its whereabouts.

(13) The supplier appears to be in a hurry to complete transaction or is willing to sell Precious Metals and Stones at arate significantly lower than their typical sale value.

(14) The supplier does not appear to understand the Precious Metals industry or lacks the appropriate equipment or finances to engage in regulated activity in the Precious Metals and Stones industry.

(15) The supplier appears to be uninterested in or uninformed about the structure or transactions of their Precious Metals business.

(16) Other indicators that may warrant closer scrutiny. For example, the supplier offers productssuch as loose diamonds that retain their wholesale value because they can be easily liquidated. The supplier may insist on offering products through non-face-to-face means (telephone, mail internet). These delivery channels may pose higher risks, as it may make it more different to identify the supplier.

8. REPORTING OF SUSPICIOUS ACTIVITY

8.1. Overview

(1) Upon receipt of a Suspicious Activity Report (SAR) from an employee or upon identifying suspicious activity or transactions, the CO/MLRO of The Company shall promptly initiate the following procedures:

(a) **Inquire and Document Circumstances:** The CO/MLRO shall conduct a thorough inquiry into the circumstances that led to the internal SAR. This includes documenting all relevant details, such as the nature of the suspicious activity, parties involved, transactional information, and any supporting documentation.

(b) **Determine the Requirement for SAR:** The CO/MLRO shall assess whether, in accordance with the UAE's Regulatory requirements, a SAR shall be submitted to the Financial Intelligence Unit (FIU). This determination shall be based on the criteria and thresholds specified by the regulatory authorities, including indicators of money laundering, terrorist financing, proliferation financing, or other illicit activities.

(c) **Submission of SAR to the FIU:** If the CO/MLRO determines that a SAR is warranted, it shall promptly prepare and submit the SAR to the FIU. The SAR shall contain comprehensive details of the suspicious activity, accompanied by supporting evidence and any additional information requested by the regulatory authorities. The submission to the FIU shall be made as soon as practicable to ensure timely reporting.

(d) **Notification to the Authorities**: Immediately following the submission of the SAR to the FIU, the CO/MLRO shall notify the relevant Authority of the filing of the SAR. This notification serves to keep the Authority informed of the reported suspicious activity and demonstrates The Company's commitment to fulfilling reporting obligations.

(2) The CO/MLRO shall maintain accurate records of all SARs, including documentation of the inquiries conducted, determinations made, and copies of SAR submissions. These records shall be securely stored in accordance with data protection and retention policies.

(3) It is imperative that the CO/MLRO treats SARs and related information with utmost confidentiality. Access to this information shall be restricted to authorized personnel involved in the investigation or required reporting processes. The confidentiality and data protection measures shall be strictly upheld in compliance with applicable laws and regulations.

(4) Regular monitoring and review of SARs, as well as the effectiveness of the reporting process, shall be conducted by the Compliance Officer/MLRO. This enables the identification of patterns, trends, or systemic issues related to suspicious activity within The Company. The information gleaned from these reviews shall be utilized to enhance the effectiveness of The Company's AML measures and reinforce the overall risk management framework.

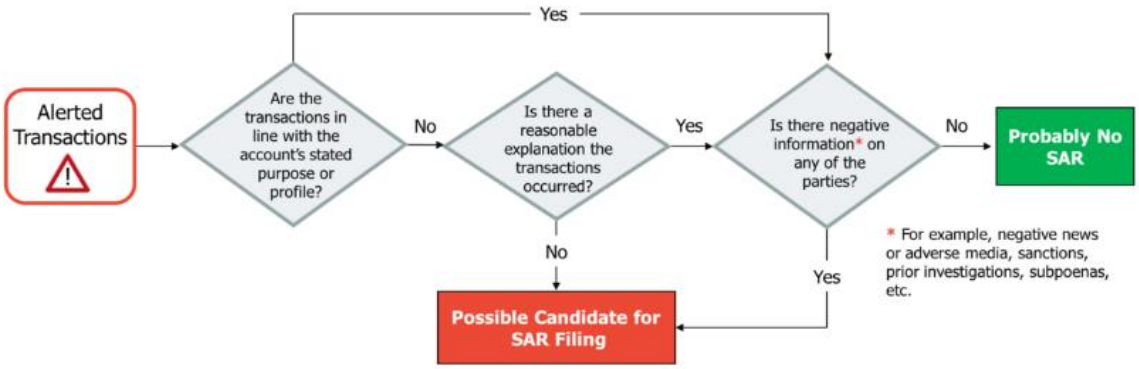
(2) By implementing robust procedures for suspicious activity reporting, The Company demonstrates its commitment to combating money laundering, terrorist financing, proliferation financing, and other illicit activities within the Precious Metals & Gold sector. These procedures align with UAE's Federal AML guidelines and regulatory requirements, fostering a culture of vigilance and compliance throughout the organization.

(3) The Compliance/MLRO shall strive to file an external STR/SAR via the GoAML platform within 24 hours of determination or as soon as reasonably possible and in line with legal and regulatory requirements. Any request received from the authority for additional information/documents via the GoAML platform shall be actioned by the MLRO promptly, without delay and in line with legal requirements and guidance. All decisions to file or not file a SAR shall be signed-off by the MLRO.

(4) Adequate guidance on filing SARs via the GoAML platform have been published by the UAE authorities and shall be referred to and complied with by the MLRO at all times. Recent guidance published can be accessed here:

- https://www.uaefiu.gov.ae/en/more/knowledge-centre/system-guides

(5) Given below is a flowchart that depicts a typical decision-making process when it comes to deciding to file an SAR with the FIU:



8.2. Tipping off

(1) Informing any person that he is being scrutinised, or that any competent authority is investigating his/her possible involvement in, suspicious activity related to money laundering is strictly prohibited.

(2) Employees shall be sensitive to these issues when considering CDD measures and take all reasonable care to avoid "tipping off".

(3) Accordingly, if The Company reasonably believes that performing CDD measures shall tip-off a Customer or potential Customer, it may choose not to pursue that process and should file an External SAR instead.

9. SANCTIONS SCREENING AND RELATED OBLIGATIONS

9.1. Sanctions Screening

(1) The Company adheres to Sanction laws and programs of various nations and intergovernmental bodies. Our compliance program includes and follows obligations and expectations such as those issued by the Central Bank of the UAE, the United Nations and the EU.

(2) The Company follows the instructions provided in the 'search notices' immediately in case the name of a party to a transaction is an exact match to a name or names in such notices issued by the Central Bank.

(3) Our sanctions compliance program is designed to ensure that The Company complies with applicable economic sanctions laws in every jurisdiction with which it may choose to trade or operate.

(4) The following procedures shall be strictly adhered to:

- Maintain logs/records related to the clearing of potential sanction matches and keep them available in the system for five (5) years.

- Screen transactions against watch/sanctions lists such as UN Security Council, Central Bank of UAE, European Union, UK's HM Treasury and US's OFAC.

- Conduct Sanctions Compliance training program for all our employees.

- Not deal with any person/entity which may result in violation of any sanctions regulations.

- Introduce written processes and procedures for the escalation and clearing of potential sanction matches.

- Regular and automatic update of the UN sanction lists within the Point of Sale or computer systems without any manual intervention.

- Immediate update of changes pertaining to addition and deletion of names in the UN Sanctions list as when such changes are announced by the UN Security Council. Should also maintain appropriate logs into the system to confirm such updates.

- In case the name of a customer is an exact match (i.e., a true match) to a name or names in the UN Sanction lists or 'search and freeze notices' issued by the Central Bank, DNFBP's shall immediately freeze the funds of such customer, shall inform the FIU along with the details of the customer and the amount of funds for further instructions. The Company shall not unfreeze such amounts without obtaining a confirmation from the FIU.

- If the name of a party to a transaction is an exact match to a name or names in 'search notices' issued by the Central bank, The Company shall immediately follow the instruction provided in such CB notices.

- Apply sanction screening against the customer's name while selling or buying PMS.

- In case of transactions conducted by a legal entity, the name of the authorized person who carried out the transaction (i.e., representative) shall be screened against sanctions lists in addition to the name of the entity and its Beneficial Owner.

- The Company strictly complies with the sanction screening requirements in case of third-party transactions.

- To require from commercial customers a separate Declaration Form confirming that their transactions have no direct or indirect relations with sanctioned countries, and they do not act on behalf of any third party in facilitating remittances/payments.

- To prohibit any transactions to and from sanctioned countries

- To report breaches of sanctions to the relevant regulatory authority

9.2. Sanctions and related obligations

(1) The Company shall have in place 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 United Nations Security Council ("UNSC")

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

(c) the Office of Foreign Assets Control (OFAC);

(d) Financial Action Task Force;

(e) Executive Office for Control and Non-Proliferation

(2) Measures in a finding that The Company shall comply with include, but are not limited to:

(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 Relevant Persons 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 ranches and subsidiaries located in a specified jurisdiction.

(3) The Company is also required to ensure compliance with obligations under UAE Cabinet Decision No. 74 of 2020 (as amended from time to time) regarding UAE sanctions. To comply with these requirements, The Company makes use of a proper screening tool at the customer on boarding stage and for ongoing screening purposes.

(4) The MLRO enters a list of names into the said screening tool (customer name, trading name, shareholders, UBOs and directors) in order to assess whether there are any sanctions hits and the customer onboarding shall proceed accordingly. The MLRO also periodically checks The Company's customer database against UNSC and UAE sanctions lists (particularly when updates to these lists are announced), to see if there are any matches.

(5) If a prospective or existing customer or transaction appears on any of the relevant sanctions lists, The Company shall notify the Authorities. The notification shall be made once The Company becomes aware and it shall include a description of the customer relationship, the activity undertaken with or on behalf of the customer and any subsequent action taken by The Company in relation to the sanctions issue.

9.3. Targeted Financial Sanctions

(1) The UAE, as a member of the United Nations, is mandated to implement UNSC Resolutions (UNSCR), including those related to the UN's sanctions regimes. Consequently, through the Cabinet Resolution No. 74 of 2020, the UAE is implementing relevant UNSCRs on the suppression and combating of terrorism, terrorist financing and countering the financing of proliferation of weapons of mass destruction, in particular relating to targeted financial sanctions (TFS). The UAE Government also applies TFS by publishing a Local Terrorism List in accordance with UNSCR 1373 (2001).

(2) The term 'targeted sanctions' means that such sanctions are imposed against specific individuals or groups, or undertakings. The term TFS includes both asset freezing without delay and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of individuals, entities, groups, or organization who are sanctioned.

(3) Financial sanctions could be by way of 'asset freezing' or 'prohibition to offer funds and services. Once implemented, these have no time limit – the freeze shall remain until the concerned party is removed from the list or an authority approves freezing cancellation. The freezing measures, including the prohibition of making funds available, apply to:

(a) Any individual, group, or entity listed in the Local (UAE) Terrorist List or listed by the UNSC.

(b) Any entity directly or indirectly owned or controlled by a listed individual or entity;

(c) Any individual or entity acting on behalf of or at the direction of any listed individual or Entity

9.4. The Company as a UAE DNFBP shall

(1) Register at the Executive Office for Control and Non-Proliferation ("EOCN") website to receive automated email notifications https://www.uaeiec.gov.ae

(a) Upon registration, automated emails shall be received as and when there are updates to the UN List or the UAE Local Terrorist List. The Company relies on these updates to check its customer database for matches

(b) The Company shall review their customer database periodically to see if there are any matches. The emails received from EOCN also require firms to complete a TFS Survey confirming whether a match (full or partial) was found. These surveys are typically completed and submitted by the MLRO, and evidence of the same is retained as part of The Company's records

(2) Undertake ongoing checks to the following databases to identify possible matches with names listed in the Sanctions Lists issued by the UN List or the UAE Local Terrorist List;

(a) Existing customer databases.
(b) Names of parties to any transactions.
(c) Potential customers.
(d) Beneficial owners.
(e) Names of individuals or entities with direct or indirect relationships.
(f) Customers before conducting any transactions or entering a business relationship with any Person.
(g) Directors and/or agents acting on behalf of customers (including individuals with power of attorney).

(3) Apply TFS (i.e., freezing measures) within 24 hours if a match with the UN List or the Local Terrorist List is identified

(4) Notify the Authority as Supervisory Authority about having applied TFS (this requirement is as per Art. 21 of the Cabinet Resolution No. 74 of 2020).

(5) Submit a Funds Freeze Report (FFR) or Partial Name Match Report (PNMR) as applicable via the GoAML portal within 5 business days from taking any freezing measure and/or attempted transactions. The Executive Office as well as the Authority receive submissions via the GoAML portal.

(6) Cooperate with the EOCN and the designated Authority in verifying the accuracy of the submitted information submitted.

(7) Implement the freezing cancellation or lifting decision, when appropriate, and/or upon receiving communication from the EOCN via GoAML, without delay (within 24 hours).

9.5. Guidelines issued by the Authorities

(1) The MLRO refers to relevant guidance issued by the UAE Authorities in relation to the above.

(2) When a Confirmed Match to a designated individual, group, or entity to the UAE Local Terrorist List or UNSC Consolidated List is identified, The Company is required to take the following actions:
(a) Freeze without delay and prohibition of making funds or other assets available or provide Services;
(b) Report measures via the GoAML platform within five business days by selecting the Fund Freeze Report (FFR);

(c) The Designated Authority and the EOCN shall receive the report;

(d) Ensure all the necessary information and documents regarding the Confirmed Match is submitted along with the FFR and any requests received for additional information/documents are promptly responded to, within stipulated timelines; and

(e) Ensure freezing measures remain in effect until the person is de-listed.

9.6. Potential Match

(1) When a Potential Match to a designated individual, group, or entity to the UAE Local Terrorist List or UNSC Consolidated List is identified, The Company is required to take the following actions:

(a) Suspend immediately any transaction and refrain from offering any funds or services;

(b) Report the Potential Match via GoAML platform by selecting the Partial Name Match Report (PNMR) within five business days;

(c) Ensure all the necessary information and documents regarding the name match is submitted and any requests received for additional information/documents are promptly responded to within stipulated timelines; and

(d) Uphold suspension measures related to the Potential Match until further instructions are received from the EOCN or the authority.

9.7. Screening obligations

(1) The Company shall undertake regular and ongoing screening on the latest Local terrorist list and UN consolidated list. Screening shall be undertaken in the following timelines:

(a) Upon any updates to the local terrorist list or UN consolidated list;

(b) Prior to on boarding new customers;

(c) Upon KYC reviews or change to a customer's information; and

(d) Before processing any transaction.

(2) The Company's internal screening process shall take into account sanctions-related risks. Where there are higher risks, The Company should respond appropriately to manage and mitigate the risks, including applying enhanced screening measures. Likewise, where the risks are lower, The Company should ensure that the screening measures are appropriate with the lower level of risk. The Company shall ensure full implementation of targeted financial sanctions in any risk scenario.

(3) The MLRO refers to relevant guidance issued by the Authority and other concerned UAE authorities in relation to the above.

(4) When a Confirmed Match to a designated individual, group, or entity to the UAE Local Terrorist List or UNSC Consolidated List is identified, The Company is required to take the following actions:

(a) Freeze without delay and prohibition of making funds or other assets available or provide services;

(b) Report measures via the GoAML platform within five business days by selecting the Fund Freeze Report (FFR). The Designated Authority and the EOCN shall receive the report;

(c) Ensure all the necessary information and documents regarding the Confirmed Match is submitted along with the FFR and any requests received for additional information/documents are promptly responded to, within stipulated timelines; and

(d) Ensure freezing measures remain in effect until the person is de-listed.

(5) When a Potential Match to a designated individual, group, or entity to the UAE Local Terrorist List or UNSC Consolidated List is identified, The Company is required to take the following actions:

(a) Suspend immediately any transaction and refrain from offering any funds or services;

(b) Report the Potential Match via GoAML platform by selecting the Partial Name Match Report (PNMR) within five business days;

(c) Ensure all the necessary information and documents regarding the name match is submitted and any requests received for additional information/documents are promptly responded to within stipulated timelines; and

(d) Uphold suspension measures related to the Potential Match until further instructions are received from the EOCN or the authority.

10. AML TRAINING AND AWARENESS

10.1. Introduction

(1) The Company provides AML training to all Employees as soon as reasonably practicable after joining and not less than annually thereafter.

(2) The form, content and objectives of the AML training programme is overseen by the MLRO and specifically addresses the core topics and objectives below.

10.2. Core topics and objectives

(1) The MLRO shall ensure that The Company's AML training:

(a) is appropriately tailored to The Company's activities, including its products, services, Customers, distribution channels, business partners and level and complexity of Transactions;

(b) indicates the different levels of money laundering risk and vulnerabilities associated with its business; and

(c) enables The Company's Employees to be able to:

(i) understand the relevant legislation relating to money laundering;

(ii) understand The Company's AML policies, procedures, systems and controls;

(iii) 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 the making of an Internal SAR to the MLRO;

(iv) recognise and deal with Transactions and activities, including how to seek and assess the information that is required for them to judge whether a person is involved in suspicious activity which may be related to money laundering or terrorist financing;

(v) understand The Company's arrangements for making an Internal SAR to the MLRO;

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

(vii) understand the roles and responsibilities of Employees in combating money laundering, such as the identity and responsibility of the MLRO; and

(viii) understand the relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions issued by government.

11. RECORD KEEPING

11.1. Objectives

(2) The Company's record keeping objectives are to ensure that:

(a) the competent authority is able to assess The Company's compliance with the UAE Regulatory requirements;

(b) any Transaction which was arranged or processed by or through The Company on behalf of a customer or other third party can be reconstructed;

(c) any Customer or third party can be identified; and

(d) The Company's can promptly satisfy any regulatory enquiry or court order to disclose information.

11.2. Records to be maintained

(1) The Company shall maintain the following records:

(a) Customer due diligence

(i) a copy of, all documents and information obtained in undertaking initial and on-going CDD; and

(ii) the supporting records (i.e. original documents and/or certified copies) in respect of a business relationship which is the subject of CDD including on-going monitoring.

(b) Suspicious activity reports

(i) internal SARs and all relevant details;

(ii) external SARs and any relevant supporting documents and findings, including internal findings and analysis; and

(iii) any relevant communications with the FIU.

(c) Risk assessment:

(i) any business risk assessment and how it was used to assist the carrying out of any Customer risk assessment; and

(ii) any Customer risk assessment and any risk rating assigned.

(d) Staff awareness and training

(i) the dates when the training was given;

(ii) the nature of the training; and

(iii) the names of Employees who received it.

(2) All such records shall be retained for at least 5 years from the date on which the notification or report was made, the business relationship ends or the Transaction is completed, whichever occurs last. If the date on which the business relationship with a customer has ended remains unclear, it shall be taken to have ended on the date of the completion of the last Transaction.

(3) Where such records are kept in electronic format, The Company shall ensure that they are readily accessible and available to respond promptly to any Authority request for information. Further, such records shall be maintained in the English language or accompanied by a salient translation, where necessary.

(4) Risk assessments shall be provided to the relevant UAE Authorities upon request.

11.3. Access to records kept outside DMCC

(1) Where the records referred to above are kept outside the DMCC, The Company shall:

(a) take reasonable steps to ensure that they are held in a manner consistent with the Rules.

(b) ensure that they are easily accessible to The Company; and

(c) that, if requested for inspection by the Authority, they are made available within a reasonable period.

(2) In such cases The Company shall:

(a) verify if there is any secrecy or data protection legislation that would restrict timely access to them by The Company, the law enforcement agencies of the U.A.E.; and

(b) where such legislation exists, promptly obtain certified copies, and keep them in a jurisdiction which allows access by those persons.

12. APPENDIX

12A: Glossary

Authorised Person	Means an Authorised Firm or an Authorised Market Institution.
Beneficial Owner	Means, in relation to a Customer, a Natural Person: (a) who ultimately controls, directly or indirectly, a Customer; (b) who, in relation to a Customer which is a Legal Person or arrangement, exercises (whether directly or indirectly) ultimate effective control over the person or arrangement, or the management of such person or arrangement; (c) who ultimately owns or has an ownership interest in the Customer, whether legally or beneficially, directly or indirectly; (d) on whose behalf or for whose benefit a Transaction is being conducted; or (e) on whose instructions the signatories of an account, or any intermediaries instructing such signatories, are for the time being accustomed to act. A person not falling into (a) or (b) is not a Beneficial Owner by reason of (c) or (d) if, having regard to a risk-based assessment of the Customer, the ownership interest is small and in the circumstances poses no or negligible risk of money laundering. In (a) to (e), a reference to a "Customer" includes a Customer account, Customer assets and the underlying Legal Person or arrangements which constitute or make up the Customer, Customer account or Customer assets.
Branch	Means a place of business within the DMCC (a) which has no separate legal personality; (b) which forms a legally dependant part of a Relevant Person whose principal place of business and head office is in a jurisdiction other than the DMCC; and (c) through which the Relevant Person carries on business in or from the DMCC.
Cabinet Resolution No. 38 of 2014	Means Federal Cabinet Resolution No. 38 of 2014 on the Implementing Regulations of Federal Law No.4 of 2002.
CTF	Means counter-terrorist financing.

Customer	(a) a person where, in relation to a business relationship between the person and a Relevant Person, there is a firm intention or commitment by each party to enter into a contractual relationship or where there is a firm commitment by each party to enter into a Transaction, in connection with a product or service provided by the Relevant Person; (b) a Client of an Authorised Firm; (c) a Member or prospective Member of, or an applicant for admission of Securities to trading on, an Authorised Market Institution; (d) in relation to a Single Family Office, a member of the Single Family; or (e) a person with whom a Relevant Person is otherwise establishing or has established a business relationship.
Designated Non-Financial Business or Profession (DNFBP)	Means: (1) The following class of persons whose business or profession is carried on in or from the DMCC (a) a real estate developer or agency which carries out Transactions with a Customer involving the buying or selling of real property; (b) a dealer in precious metals or precious stones; (c) a dealer in any saleable item of a price equal to or greater than $15,000; (d) a law firm, notary firm, or other independent legal business; (e) an accounting firm, audit firm or insolvency firm; (f) a Company Service Provider; or (g) a Single Family Office. (2) A person who is an Authorised Person or an Auditor is not a DNFBP.
Employee	Means an individual: (a) who is employed or appointed by a perso connection with that person's business, whether under a contract of service or for s (b) whose services, under an arrangement between that person and a third party, are placed at the disposal and under the control of that person.
Enhanced Customer Due Diligence	Means undertaking Customer Due Diligence and the enhanced measures
FATF	Means the Financial Action Task Force, i.e. the inter-governmental body whose purpose is the development and promotion of

	international standards to combat money laundering and terrorist financing.
FATF Recommendations	Means the publication entitled the "International Standards on Combatting Money Laundering and the Financing of Terrorism and Proliferation" as published and amended from time to time by FATF.
Federal AML legislation	Means all UAE Federal Laws and their implementing regulations relating to money laundering, terrorism financing and the financing of unlawful organisations, as well as sanctions compliance, including Federal Law No. 4 of 2002, Federal Law No. 1 of 2004, Federal Law No. 9 of 2014 and Cabinet Resolution No 38 of 2014.
Federal Law No.1 of 2004	Means UAE Federal Law No.1 of 2004 regarding Combating Terrorism Offences.
Federal Law No. 4 of 2002	Means UAE Federal Law No. 4 of 2002 on combatting the Crimes of Money Laundering and Terrorism Financing.
Federal Law No. 9 of 2014	Means UAE Federal Law No. 9 of 2014 amending Federal Law No. 4 of 2002.
FIU	Means the UAE Financial Intelligence Unit
Governing Body	Means the board of directors, partners, committee of management or other governing body of: (a) a Body Corporate or Partnership; or (b) an unincorporated association carrying on a trade or business, with or without a view to profit.
Legal Person	Means any entity other than a Natural Person that can establish a Customer relationship with a Relevant Person or otherwise own property. This can include companies, bodies corporate or unincorporate, trusts, foundations, anstalten, partnerships, associations, states and governments and other relevantly similar entities.

Member	A person admitted as a member of an Authorised Market Institution in accordance with its Business Rules.
MLRO	Means the Money Laundering Reporting Officer
Natural Person	Means an individual.
Person	Means a natural or Legal Person.
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 UAE 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, or 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, but not middle ranking or more junior individuals in these categories.
Public Listed Company	Has the meaning given in Article 97(2) of the Regulatory Law 2004.
Relevant Person	Means (a) an Authorised Firm other than a Credit Rating Agency; (b) An Authorised Market Institution; (c) a DNFBP; or (d) an Auditor.
Senior management	Means, in relation to a Relevant Person every member of the Relevant Person's executive management and includes: (a) for a DMCC entity, every member of the Relevant Person's Governing Body; (b) for a Branch, the person or persons who control the day to day operations of the Relevant Person in the DMCC and would include, at a minimum, the SEO or equivalent, such as the managing director; or (c) for an Auditor, every member of the Relevant Person's executive management in the U.A.E.

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 Customer's funds which relate to a Transaction or service and includes how such funds are connected to a Customer's Source of Wealth.
Source of Wealth	Means how the Customer's global wealth or net worth is or was acquired or accumulated.
Suspicious Activity Report (SAR)	Means a report in the prescribed format regarding suspicious activity (including a suspicious transaction) made to the FIU under Rule 13.3.1(c).
Transaction	Means any transaction undertaken by a Relevant Person for or on behalf of a Customer in the course of carrying on a business in or from DMCC
Unlawful organisation	Means an organisation the establishment or activities of which have been declared to be criminal under Federal AML legislation.

12B: Internal Suspicious Activity / Transactions Report

DETAILS OF CUSTOMER
Full name of Customer:
Customer account number, if any:
Name of Customer's representative, if any:
Current or last known address:
Phone or other contact details:
Customer's occupation or business:
Passport or identity card number:
Nationality / Place of business or incorporation:
DETAILS OF SUSPICION
Nature and amount of suspected transactions:
Details of any connected accounts:

Reason for suspicion:
NEXT STEPS (MITIGATION)
Instructions of the MLRO to the person making the report:

EMPLOYEE:		**CO/MLRO**	
Name:		**Name:**	
Signature:		**Signature:**	
Date:	**Time:**	**Date:**	**Time:**

IMPORTANT NOTE: Do not tip-off! Under Article 16 Federal Law No.4 of 2002 it is a serious offence (punishable by law) to inform any person that his transaction is being scrutinised, or that any competent authority is investigating his/her possible involvement in, suspected money laundering operations.