Anti-Money Laundering and Combatting the Financing of Terrorism Policies and Procedures

Honesty | Integrity | Respect | Transparency

Company name: Avantaa Gold Jewellery L.L.C
Version number: 1.0
Document owner: Avantaa Gold Jewellery L.L.C
Version description: New policy created

Contents

1. Definitions and Abbreviations

Definitions and Abbreviations	
AML	Anti-Money Laundering
CAML Committee	Compliance and Anti-Money Laundering Committee CBUAE
CDD	Customer Due Diligence
CID	Customer Identification Documents
CFT	Counter-Terrorism Financing or Combating Financing of Terrorisı
CP	Customer Profile
DNFBP	Designated Non-Financial Businesses and Professions
DPEP	Domestic Politically Exposed Person
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FPEP	Foreign Politically Exposed Person
HIO	Heads of International Organizations
ID	Identity Document
KYC	Know Your Customer
LOA	Letter of Authorization
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
NRA	National Risk Assessment
OFAC	Office of Foreign Assets Control (USA)
PEP	Politically Exposed Person
PoA	Power of Attorney
Retention Period	The record keeping requirements as set out in the Standards (defin below), being 5 years from the date of the last transaction.
SDN	Special Designated Nationals
STR	Suspicious Transaction Report
TF	Terrorism Financing
TL	Trade License
UAE	United Arab Emirates
UBO	Ultimate Beneficial Owner
UNSC	United Nations Security Council
EU	European Union
FIU	Financial Intelligence Unit
FT	Financing Terrorism
RCA	Relative and Close Associate
OECD	Organization for Economic Co-operation and Development
PMS	Precious Metals and Stones
SAR	Suspicious Activity Report

2. Introduction

Avantaa Gold Jewellery L.L.C is a Non-Manufactured Precious Metal trading company based in Dubai, United Arab Emirates. With a strong foundation built on the extensive experience of our founder, we are committed to providing high-quality, exquisite gold bullion bars to discerning customers.

Operating under the esteemed license no. **1042017** issued by Dubai Economy and Tourism. We are subject to the regulatory oversight of the Ministry of Economy. This ensures that our business practices adhere to the highest standards of transparency, ethics, and compliance with local and international regulations.

Our office is in Office 204, 2nd Floor, Gold House Building, Gold Souk, Deira, Dubai, UAE positions us at the heart of the city's vibrant gold trade. This prime location allows us to efficiently connect with suppliers, manufacturers, and customers from the UAE and around the world.

Our entity has registered for Value added Tax under Federal Decree Law No.13 of 2016 with Federal Tax Authority with the TRN No.100475757900003.

Business Model Overview

Our company specializes in trading precious metals, jewellery from reputable sources globally and selling them wholesale to registered entities within the UAE. Our supply chain involves importing from legally recognized entities both within and outside the UAE, ensuring compliance with relevant regulations.

Avantaa Gold Jewellery L.L.C 's Commitment:

We, **Avantaa Gold Jewellery L.L.C** steadfastly committed to upholding the highest standards of ethical conduct and regulatory compliance. We are dedicated to adhering to all applicable laws and regulations of the United Arab Emirates, with a particular focus on Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) laws and regulations in AML/CFT Law 20 of 2018 and AML/CFT Decision 10 of 2019.

Our commitment to AML/CFT compliance is unwavering. We have implemented robust AML framework by creating policies and procedures to mitigate risks associated with financial crime. These measures include:

- **AML/CFT Program**
- **Know Your Customer (KYC) Procedures**
- **Customer Due Diligence (CDD)**
- **Transaction Monitoring**
- **Suspicious Transaction Reporting (STR)**
- **Record Keeping**
- **Promptly apply directives of Competent Authorities for implementing UN Security Council decisions under Chapter 7 of the UN Convention for the Prohibition and Suppression of the FT and Proliferation.**

Our company owners and management team are deeply committed to upholding the highest standards of integrity and transparency. We have a zero-tolerance policy for any deviation from these principles. We will continue to invest in our compliance program to ensure that We remain at the forefront of AML/CTF best practices.

By adhering to these principles, we aim to contribute to a secure and transparent financial system in the United Arab Emirates.

All partners and employees of the firm are under an obligation and duty to comply with the above. This policy & any related procedures aim to help partners and staff fulfil these responsibilities by providing a clear framework, along with setting out the firm's key principles and obligations.

Failure to fulfil these responsibilities may result in disciplinary action and may also result in criminal sanctions for the staff involved. Breaches may also be reportable to our AML Supervisor (Ministry of Economy), which may result in professional disciplinary action.

VERSION CONTROL:

Date	Change	Remarks
11TH JUL 2025	New Policy Created	

This policy document is reviewed and approved by our senior management.

Reviewed and approved by

Mr. Rameshkumar Girdharlal Shah

P O BOX 1853 DUBAI - U.A.E. AVANTAA GOLD JEWELLERY L.L.C

Date: 11/7/2025

3. Purpose and Scope of these Policies & Procedures

The purpose of these Anti-Money Laundering and Combating the Financing of Terrorism and the Financing of Illegal Organisations policy is to provide guidance and assistance in order to assist their better understanding and effective performance of their statutory obligations under the legal and regulatory framework in force in the United Arab Emirates. This policy applies to all members of their boards of directors, management and employees, and counterparties who are registered inside and outside the UAE.

4. AML Legislative Framework

The principal AML/CFT legislation within the State is Federal Decree-Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations (the "AML-CFT Law" or "the Law") and implementing regulation, Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations (the "AML-CFT Decision" or "the Cabinet Decision. The following legislative laws are in place in the UAE regarding the AML/CFT procedures

- Cabinet Decision No. (74) of 2020 regarding the terrorist list system and the implementation of Security Council resolutions related to preventing and suppressing terrorism and its financing
- Cabinet Decision No (109) of 2023 on regulating the procedures of the beneficial owner procedures
- Federal Decree law No. (26) of 2021 To amend certain provisions of Federal Decree-law No. (20) of 2018, on Anti-Money laundering and combating the financing of terrorism and financing of illegal organisations
- Cabinet Resolution No. (71) of 2024 regulating violations and administrative penalties imposed on violators of procedures for confronting money laundering and combating the financing of terrorism
- Cabinet Resolution No. (132) of 2023 Concerning the Administrative Penalties against Violators of The Provisions of the Cabinet Resolution No. (109) of 2023 Concerning the Regulation of Beneficial Owner Procedures.

5. AML/CFT national Strategy Framework

The UAE is deeply committed to combating money laundering and the financing of terrorism and illegal organisations. To this end, the Competent Authorities have established the appropriate legislative, regulatory and institutional frameworks for the prevention, detection and deterrence of financial crimes, including ML/FT. They also continue to work towards reinforcing the capabilities of the resources committed to these efforts, and towards improving their effectiveness by implementing the internationally accepted AML/CFT standards recommended and promoted by FATF, MENAFATF and the other FSRBs, as Well as by the United Nations, the World Bank and the International Monetary Fund (IMF).

The pillars of the National Strategy, together with their strategic priorities are summarised in the table below

National AML/CFT Strategic Pillars	Strategic Priorities
Legislative & Regulatory Measures	Increase effectiveness and efficiency of legislative and regulatory policies and ensure compliance
Transparent Analysis of Intelligence	Leverage the use of financial databases and the development of information analysis systems to enhance the transparent analysis and dissemination of financial intelligence information
Domestic and International Cooperation & Coordination	Promote the efficiency and effectiveness of domestic and international coordination and cooperation with regard to the availability and exchange of information
Compliance and Law Enforcement	Ensure the effective investigation and prosecution of ML/FT crimes and the timely implementation of TFS

6. Statutory Obligations for DPMS

The AML-CFT Law and the AML-CFT Decision set out the minimum statutory obligations of supervised institutions as follows:

a. To identify, assess, understand risks (AML-CFT Law Article 16.1(a), AML-CFT Decision Article 4.1);
b. To define the scope of and take necessary due diligence measures (AML-CFT Law Article 16.1(b), AML-CFT Decision Article 4.1(a) and 2);
c. To appoint a compliance officer, with relevant qualification and expertise and in line with the requirements of the relevant Supervisory Authority (AML-CFT Decision Article 21, 44.12);
d. To put in place adequate management and information systems, internal controls, policies, procedures to mitigate risks and monitor implementation (AML-CFT Law Article 16.1(d), AML-CFT Decision Article 4.2(a));
e. To put in place indicators to identify suspicious transactions (AML-CFT Law Article 15, AML-CFT Decision Article 16);
f. To report suspicious activity and cooperate with Competent Authorities (AML-CFT Law Article 9.1, 15, 30, AML-CFT Decision Article 13.2, 17.1, 20.2);
g. To promptly apply directives of Competent Authorities for implementing UN Security Council decisions under Chapter 7 of the UN Convention for the Prohibition and Suppression of the FT and Proliferation (AML-CFT Law Article 16.1(e), AML-CFT Decision Article 60);
h. To maintain adequate records (AML-CFT Law Article 16.1(f), AML-CFT Decision Article 7.2, 24).

7. Basic Principles to Combat ML/TF/PF

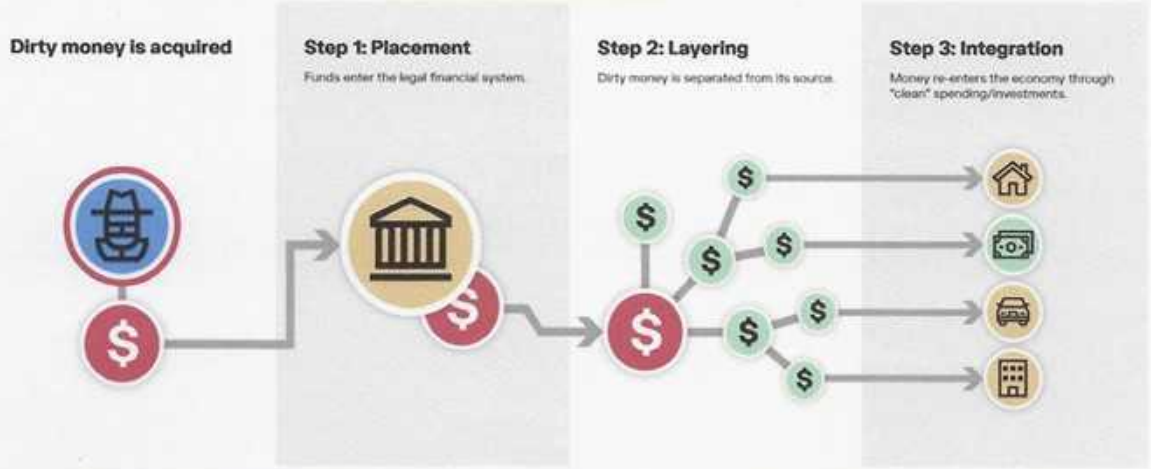
7.1. Money Laundering

7.1.1. Definitions:

The AML-CFT Law defines money laundering as engaging in any of the following acts wilfully, having knowledge that the funds are the proceeds of a felony or a misdemeanour (i.e., a predicate offence):

- Facilitating the transfer or movement of proceeds or conducting any transaction which results in concealing or disguising their Illegal source;
- Concealing or disguising the true nature, source or location of the 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 escape punishment.

7.1.2. Stages of Money Laundering



7.2. Terrorist Financing

7.2.1. FATF

Terrorist financing is the financing of terrorist acts and/or of terrorists and terrorist organizations.

7.2.2. Terrorist Organization

The term **terrorist organization** refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organizes or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

7.2.3. **Terrorist Financing –**

To provide, collect, ensure or transfer property, by any means, directly or indirectly, to any association, authority, organization, center, group, gang or any person to which apply the provisions of Federal Law No. 7 of 2014 on Combating Terrorist Crimes, whether such property is from licit or illicit source, is to be used, in full or in part, to carry out terrorist acts or not, and whether such terrorist acts have taken place or not.

7.2.4. **Stages of Terrorist Financing**

Raising Funds – Self funding from legitimate sources, through social media and crowd funding, through Non-Profit Organizations and Criminal Activity

Moving Funds – Cross-Border movement of funds, Banking system, Money Service Business and Hawala, and through new payment systems (stored value cards, virtual currencies etc.)

Using Funds – For Operational Use (weapons and explosives, training and travel), for organizational use (terrorist network maintenance, propaganda/radicalization, charity work etc.)

7.3.Proliferation Financing

Proliferation is the spread of nuclear, radiological, chemical or biological Weapons; their means of delivery such as missiles, rockets and other unmanned systems, as Well as related materials, such as WMD-sensitive materials, equipment and technology. If appropriate safeguards are not established, maintained and enforced sensitive materials, technology, services and expertise can become accessible to individuals and entities seeking to use them in WMD programmes. They can also become accessible by terrorists who are pursuing chemical, biological, radiological or nuclear (CBRN) capabilities.

The financial elements of a WMD programme can be divided into three stages:

- Raising of funds
- Obscuring of funds
- Shipping of necessary items

8. Financial Action Task Force (FATF) Standards

The Financial Action Task Force (FATF) leads global action to tackle money laundering, terrorist and proliferation financing. The 40-member body sets international standards to ensure national authorities can effectively go after illicit funds linked to drugs trafficking, the illicit arms trade, cyber fraud and other serious crimes. The FATF researches how money is laundered and terrorism is funded, promotes global standards to mitigate the risks, and assesses whether countries are taking effective action. In total, more than 200 countries and jurisdictions have committed to implement the FATF's Standards as part of a co-ordinated global response to preventing organised crime, corruption and terrorism. Countries and jurisdictions are assessed with the help of nine FATF Associate Member organisations and other global partners, the IMF and World Bank.

The FATF's decision-making body, the FATF Plenary, meets three times per year and holds countries to account if they do not comply with the Standards. If a country repeatedly fails to implement FATF Standards then it can be named a Jurisdiction under Increased Monitoring or a High-Risk Jurisdiction. These are often externally referred to as "the grey and black lists". The FATF was established in 1989 and is based in Paris.

The 40 Recommendations are divided into seven distinct areas:

- AML/CFT Policies and coordination
- Money laundering and confiscation
- Terrorist financing and financing of proliferation
- Preventive measures
- Transparency and beneficial ownership of legal persons and arrangements
- Powers and responsibilities of competent authorities and other institutional measures
- International cooperation

9. Money Laundering and Financing of Terrorism Risk Assessment

Avantaa Gold Jewellery L.L.C is aware of the ML/FT risks inherent in the products and services being undertaken by the business and is dedicated to managing and mitigating these risks effectively.

In this regard, the Compliance & AML Department undertakes an Institutional Risk Assessment to identify significant risk areas, recommending a risk-based allocation of resources to the highest risk areas, and creating a pre-emptive long-term plan, as well as implementing action plans for managing the risks identified.

Avantaa Gold Jewellery L.L.C acknowledges the regulatory expectations in all jurisdictions on the adequacy of internal controls, governance and risk mitigating measures that should be present throughout its business. Avantaa Gold Jewellery L.L.C strives to demonstrate the effectiveness of managing and mitigating these risks through the first, second and third lines of defense, including, risk management. This risk assessment is based on the following factors:

- Size and nature of our business
- The Market in which Avantaa Gold Jewellery L.L.C operates
- Number and type of Counterparties (Suppliers, Buyers, etc.)
- Overview of number and type of Customers
- Products/Services provided to these customers
- Countries where these customers are active (Geography/Jurisdictions)
- Transaction Patterns
- Delivery Channels
- Employees

10. Three Lines of Defense

The governance is a fundamental component of an effective Anti-Money Laundering (AML) program. It establishes the framework for how our organization will manage and oversee its AML activities, ensuring compliance with relevant laws and regulations.

Key Elements of an AML Governance Policy:

1. Board and Senior Management Oversight:

Responsibility: The board and senior management are responsible for overseeing the AML program and ensuring its effectiveness.

Accountability: They are accountable for any failures in the AML program.

- AML Committee:

Establishment: The establishment of a dedicated AML committee to provide oversight and guidance under the supervision of company owner and compliance team.

We have three lines of defense to ensure our AML/CFT program is working properly.

1st Line of Defense **FLA/Sales/Operations**

- They are our company's 1st Line of defense since they are facing the customers and doing the on boarding and transactions. So the 1st line of defense should be properly trained how to do proper KYC, CDD, EDD process and SAR/STR process along with Sanction screening.

2nd Line of Defense **MLRO/Compliance Team**

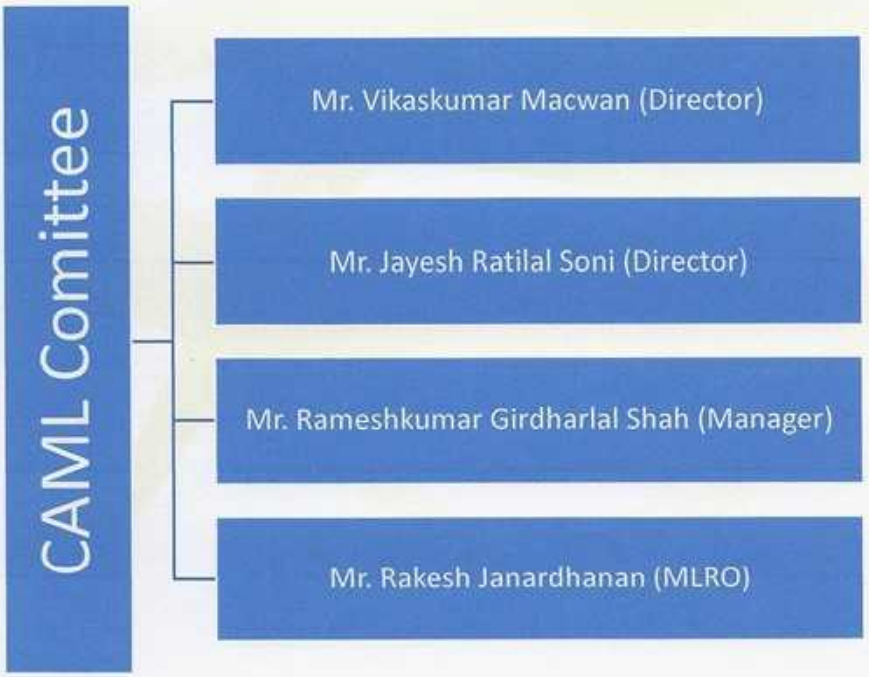
- This 2nd Line of defense consists our compliance team and MLRO, those are monitoring the activities of 1st Line staff and verify the documents and informations obtained by them from the customer. 2nd Line staffs also well trained to identify, assess and report of customer transactions and KYC.

3rd Line of Defense **Independent/Internal Audit**

- The auditors appoints by us are completely indepdent from our company, they will assess, check and report the activities and documents related to AML/CFT programme and process to our senior managment. They will act like 3rd line of defense of our company.

11. Corporate Governance, Roles and Responsibilities

11.1. The Compliance and Anti-Money Laundering Committee (CAML Committee)



11.2. Board of Directors

The Board of Directors is the governing and policy making body for the company. The Board of directors have overall responsibility for approving strategies, policies, organizational structure and are legally empowered to take decisions in relation to the business. The Board of Directors provides governance, guidance and oversight across the business from an AML & CFT perspective.

11.3. Senior Management

We strongly believe that strong AML/CFT governance of our company is lying in senior management involvement and their accountability. Senior Management are ultimately responsible for the quality, strength and effectiveness of the DNFBP's AML/CFT framework, as Well as for the robustness of its compliance culture.

- These responsibilities of our senior management Implementation of governance, control, and operating systems
- Approval of internal policies, procedures and controls
- Oversight of the AML/CFT compliance programme
- Application of the directives of Competent Authorities can be grouped broadly into categories.

11.4. Compliance Officer/MLRO

The Compliance Officer (CO) situated at Avantaa Gold Jewellery L.L.C is responsible for the formation, implementation and management of Avantaa Gold Jewellery L.L.C's AML/CFT compliance function. The CO reports directly to the Board of Directors on matters related to AML & CFT, compliance and risk management and has unrestricted access to all information in order to perform this role effectively without interference.

AML/CFT Programme Management:

MLRO should ensure the quality, strength and effectiveness of the of our company AML/CFT programme. As such, the MLRO should be a stakeholder with respect to the our company's ML/FT business risk assessment, and the overarching AML/CFT risk mitigation framework, including its AML/CFT policies, controls and CDD measures. The MLRO is in charge of informing and reporting to senior management on the level of compliance and report on that to the relevant Supervisory Authority. MLRO is responsible for updating recent changes/modifications given by regualtory in UAE as Well as FATF, MENAFATF and other AML watchdogs.

ML/FT Reporting :

MLRO is responsbole for reviewing, scrutinizing and reporting of DPMSR/STRs/FFR/PNMR/HRC/HRCA/AIF/AIFT . In this capacity, the MLRO is ultimately responsible for the detection of transactions related to the crimes of money laundering and the financing of terrorism and of illegal organisations, for reporting suspicions to the FIU, and for cooperating with the Competent Authorities in relation to the performance of their duties in regard to AML/CFT.

AML/CFT Training and Development:

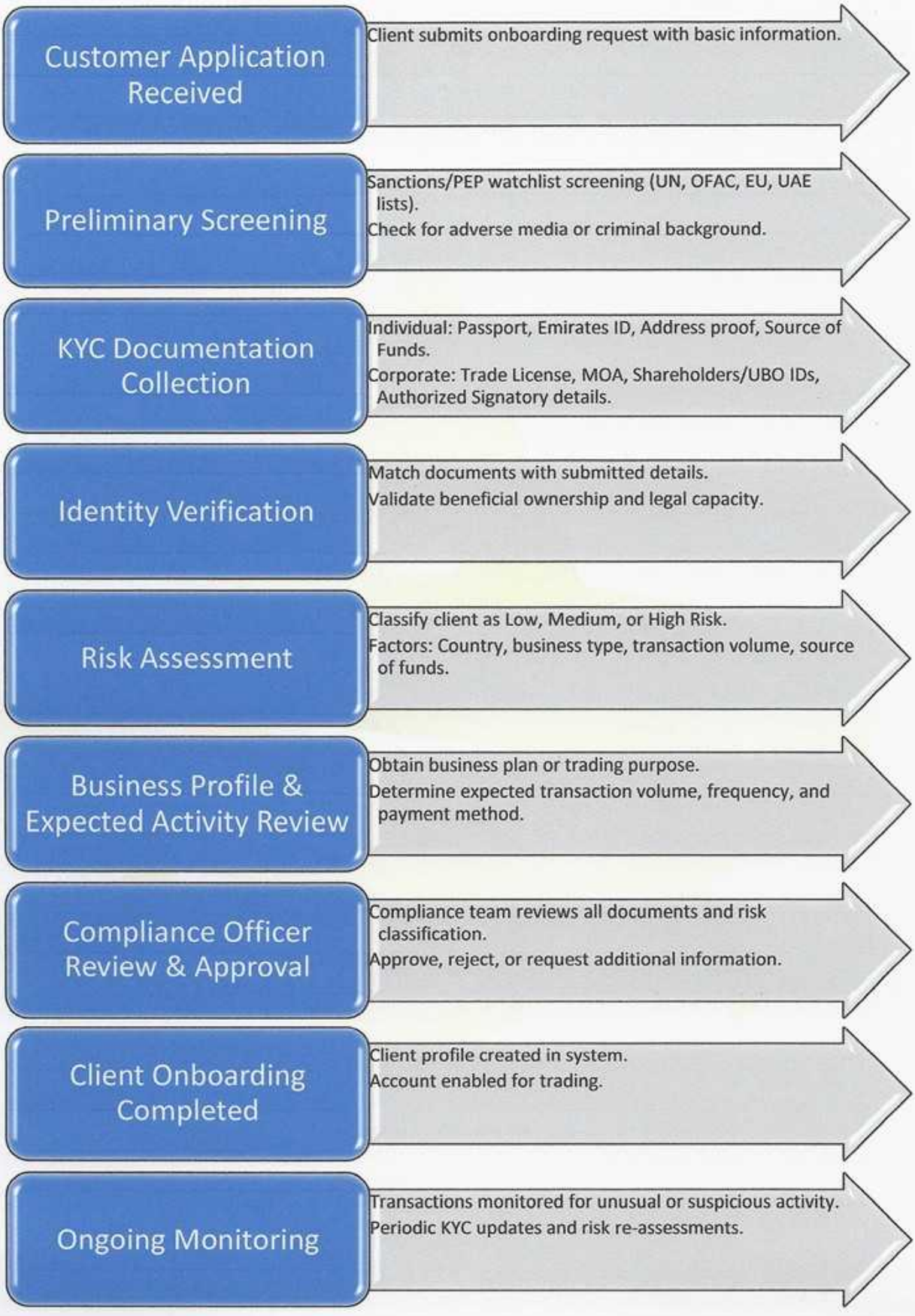
Our company's MLRO is responsible for educating and updating senior management/BOD/Owners in respect of changes in AML compliance process or procedure. Timely update the changes implemented by supervisory body or regulatory authority to the senior management and accordingly set the company AML policy and procedures. And also ensure that the staff are Well-qualified, Well-trained, Well-equipped, and Well-aware of their responsibility to combat the threat posed by ML/FT.

The role of the Compliance Officer will not be combined with any other responsibilities within the business to ensure independence and any potential conflict of interest.

The CO is principally responsible for the following functions:

- Design and implementation of an appropriate compliance program for Avantaa Gold Jewellery L.L.C to ensure compliance with all applicable legislation, regulation and international best practice at all times and ensuring the compliance program is reviewed and updated on an annual basis and these AML Policies and Procedures reflect such updates
- Central reference point for the oversight of all Avantaa Gold Jewellery L.L.C's activities relating to the prevention and detection of money laundering and terrorism financing, reporting line directly to the Board of Directors and the CAML Committee
- Acting as the prime point of contact with regulatory authorities, enforcement authorities and other competent authorities and correspondents on issues relating to Avantaa Gold Jewellery L.L.C's compliance function
- Ensures proper implementation and compliance with all relevant AML & CFT and sanction policies, procedures and practices across the business units, subsidiaries and affiliates, in accordance with these AML Policies and Procedures up to the extent allowed by law and regulation in each jurisdiction.
- To manage and direct the team members of the Compliance & AML Department ensuring adequate training of all employees on AML & CFT, sanctions, fraud and financial crimes in accordance with these AML Policies and Procedures
- Communication of key AML & CFT issues with senior management
- Providing periodical/specific reports to the Board of Directors through the CAML Committee on a regular basis.
- Preparation of an Annual Compliance Report regarding implementation of any AML & CFT regulations and procedures.
- Ensuring appropriate AML & CFT controls and monitoring systems are in place to identify high risk or suspicious transactions
- Manage, evaluate and test all Avantaa Gold Jewellery L.L.C AML & CFT systems, processes and these AML Policies and Procedures on a regular basis to ensure adequacy and relevance to legislation and regulation and to ensure appropriate and timely mitigation of any gaps or issues identified.
- Ensuring that any infractions identified by internal or external audits or examinations conducted by regulators or other third-party auditors are remedied in a timely fashion.
- Central point for filing of all SAR/STRs in the business, to analyze and take appropriate decisions on disclosures for submission to the FIUs in a timely manner
- Ensuring all compliance records demonstrating adherence to these AML Policies and Procedures are maintained in accordance with the Retention Period.

12. Customer Onboarding Flow:



13. Customer Due Diligence (CDD)

13.1. Robust customer due diligence—comprising Identification (ID), Verification (VR), and Know Your Customer (KYC)—is a critical safeguard against money laundering and terrorist financing. These measures represent the foundational step in Avantaa Gold Jewellery L.L.C's onboarding procedures and internal controls and are strictly mandatory for all clients.

13.2. Avantaa Gold Jewellery L.L.C shall establish, document, and maintain a Customer Identification Program (CIP) tailored to the nature, scale, and complexity of its PMS trading operations. This program will form an integral part of the company's AML/CFT compliance framework and shall incorporate, at a minimum, all required elements outlined in the approved KYC Checklist.

13.3. As part of the onboarding process, Avantaa Gold Jewellery L.L.C shall obtain and maintain reliable, documents to confirm the full and true identity of the customer, including their Ultimate Beneficial Owner (UBO), authorized representatives, legal domicile, capacity, source of funds, intended nature of the business relationship, and purpose of the transactions. This will apply to both occasional and ongoing clients. An initial assessment will be made based on document verification, background screening, business plan review, and expected transactional profile to determine whether the application is to be approved, declined, or held pending further information.

13.4. All prospective clients shall be informed of Avantaa Gold Jewellery L.L.C's clear policy that it will not establish business relationships with individuals or entities that fail to provide satisfactory identification and due diligence documentation. In cases where identification cannot be verified or is deemed suspicious, enhanced due diligence (EDD) procedures will be initiated. All steps, findings, and decisions arising from these procedures must be thoroughly documented.

13.5. If at any point during the business relationship Avantaa Gold Jewellery L.L.C identifies discrepancies or has reasonable grounds to doubt the accuracy or legitimacy of client-provided information—whether relating to identity, beneficial ownership, or changes not previously disclosed—it shall immediately initiate further verification procedures. These may include:

- Escalation and referral to relevant investigative or regulatory authorities; and
- A comprehensive review of any disciplinary history or prior regulatory sanctions associated with the customer or UBO.

13.6. The Customer Identification Program must include clearly defined procedures for instances where the Compliance Monitoring Team is unable to reasonably verify a customer's identity. These procedures shall address:

- Conditions under which business relationships must not be initiated or continued;
- Parameters for allowing limited transactions while identity verification is pending; and
- Circumstances warranting the filing of a Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR).

13.7. Avantaa Gold Jewellery L.L.C shall ensure customers are adequately notified that identity and background information is being requested for the purpose of compliance with applicable AML/CFT regulations and internal risk management procedures.

In cases where a client is unwilling or fails to provide the required KYC documentation, or demonstrates reluctance to comply with onboarding protocols, Avantaa Gold Jewellery L.L.C shall terminate or decline the relationship, classify the party as a High-Risk Client, and report the case to the appropriate authority through an STR. Additionally, such clients will be flagged for enhanced ongoing monitoring and internal escalation.

14. Enhanced Due Diligence (EDD)

A High-Risk Customer will be one who presents a higher-than-normal adverse potential risk of involvement in money laundering or financing of terrorism or financing of illegal organization or any other matter that Senior Management or the Compliance Officer consider to be significant.

To address the elevated risk associated with such clients, Enhanced Due Diligence (EDD) procedures shall be applied in addition to standard onboarding and monitoring requirements. The necessity and extent of EDD will be determined by Senior Management, in coordination with the Compliance Officer, based on the risk profile of the client and their intended business relationship with Avantaa Gold Jewellery L.L.C.

Due to the varied nature of high-risk classifications, EDD measures must be tailored on a case-by-case basis, ensuring that the level of scrutiny corresponds with the specific risk indicators presented.

EDD Documentation Requirements

Where a customer is flagged as high risk, Avantaa Gold Jewellery L.L.C may require submission of one or more of the following documents to assess the client's internal controls, financial standing, and regulatory compliance:

- Audited Financial Statements
- Tax Returns
- Recent Bank Statements
- AML/CFT Policy of the Customer
- Bank Reference Letter
- Dubai Good Delivery / LBMA / RIC Certifications
- Independent Assurance / Compliance Review Reports
- Detailed Business Profile

These documents, whether collected in full or partially, support the compliance team in conducting deeper evaluations, enabling more informed decisions about whether to engage in business with the client.

If the results of the EDD process do not provide sufficient assurance, Avantaa Gold Jewellery L.L.C reserves the right to decline the business relationship, and the customer will not be onboarded.

Approval Process

All High-Risk Customer files must receive explicit approval from Senior Management prior to activation of the trading relationship.

Scenarios Requiring Enhanced Due Diligence Avantaa Gold Jewellery L.L.C shall conduct EDD in, but not limited to, the following scenarios:

- Customers incorporated or operating in jurisdictions classified as high-risk by international or UAE authorities.
- Individuals identified as Politically Exposed Persons (PEPs) or those with close association to PEPs.
- Transactions or customer behaviour's that appear suspicious, irregular, or inconsistent with declared profiles.
- Red flags raised due to compliance rule violations, transaction monitoring triggers, or screening hits.

These risk triggers and EDD procedures are reviewed and updated periodically.

15. Periodic Reviews

Periodic reviews are conducted annually or upon the expiry date of ID documents provided during the customer onboarding process (whichever is the earlier). The customer will not be able to conduct business with Avantaa Gold Jewellery L.L.C unless updated with renewed identification documents. 12 months after the customer onboarding and on a rolling 12-month basis, customer information and Identification documents is verified to ensure the information held in the system is accurate.

16. Customer Profile (CP)

CP is a document completed by the customer, providing us with the best possible information about their business and its activities and is designed to assist our employees in ensuring that the customer and their related transactions are not involved directly or indirectly, in any form of money laundering, terrorist financing or financing of proliferation.

The CP should always contain the most up to date KYC information and supporting documents and its creation is mandatory for all corporate customers during the customer on-boarding process.

16.1. Corporate Customers/Legal Entities KYC Requirements

- A duly completed and signed Corporate Onboarding form, should be submitted with all other required on-boarding documents.
- Ownership structure of the legal entity must be collected including the purpose and nature of the intended business relationship.
- Collect copies of valid permissions/licenses of the entity from competent authorities to carry out the business (examples: certificate of incorporation, trading license or equivalent, or other competent authorities where applicable).
- Identification documents of Ultimate Beneficial Owners (UBO) must be verified and copies retained.
- Apply sanction checks and internet searches on the name of the legal entity, Ultimate Beneficial Owners, group companies, subsidiaries and the names of representatives of the legal entity who are authorized to carry out transactions on its behalf.
- Apply PEP checks on Ultimate Beneficial Owners and where the Ultimate Beneficial Owner is a PEP, we must collect the information about the source of wealth of such UBO and the business relationship must only be entered into after approval has been obtained from the Board of Directors.
- Information of source of funds which should be verified.
- Obtain the reason/purpose for the transaction and review whether it matches with the customer profile and is a valid/economic reason for transmitting such funds.

17. Ongoing Customer Due Diligence

CDD/EDD is not a 'one-off' process and should be reviewed periodically for all customers to obtain further information on the profile of the customer. Where the accuracy of information available is in doubt, another round of CDD/EDD procedures should be undertaken.

While entering into the relationship, the purpose and intended nature of the business relationship must be established. This should include understanding the ownership and control structure of the customer (beneficial ownership and ultimate control), as well as ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions conducted are consistent with the Avantaa Gold Jewellery L.L.C knowledge of the customer, its business and risk profile.

Where warranted, enhanced due diligence should be conducted especially where customer is in high-risk category and/or where suspicion prevails.

Aside from the periodic reviews, Avantaa Gold Jewellery L.L.C ensures that CDD information is updated upon certain trigger events which include:

- when a significant transaction is about to take place
- when a material change occurs in the way the customer's account is operated
- when the customer's documentation standards change substantially or
- when there is lack of sufficient information about the customer concerned and
- when re-activating a dormant/inactive onboarded customer profile.

18. Identification and Verification of a Beneficial Owner

(FATF Recommendation Nos. 24-25)

"Beneficial owner" refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. Avantaa Gold Jewellery L.L.C is aware of the obligation to verify the identity of a beneficial owner/s and will take reasonable measures to satisfy that it knows the identity of the beneficial owner/s (having 5% share or more) of corporate customers.

19. Risk Based Approach

19.1. A risk-based approach is one of the most effective ways to protect against money laundering and terrorist financing. It is imperative to understand that certain risks associated with various elements of a customer's profile may be indictive of potential criminal activity. This may include geographical and jurisdictional issues, business and product types, distribution channels and prevailing transaction types and amounts.

19.2. Customers will be reviewed, assessed, and allocated an appropriate level of risk of money laundering, divided into – High, Medium or Low Risk.

- High risk customer will be subject to enhanced levels of due diligence that go beyond the core policies and principles contained in this policy.

- Medium risk customers will be subject to the core policies and procedures contained within this policy.
- Low risk customers may be subject to certain flexibility within the policies and procedures contained within this policy. However, great care should be exercised to ensure that the Company continues to meet its legal obligations.

19.3. Although it is generally accepted that failure to provide satisfactory due diligence documentation might be indicative of a money laundering concern, it is also recognized that due to the geographic diversity of businesses, on occasion, it might prove difficult or impossible to obtain documentation that exactly meets the criteria set out within this policy.

19.4. If the situation mentioned in the Clause above occurs, and there are no reasons to suspect money laundering, the customer documentation should be communicated to senior management and/or the Chief Compliance Officer, together with an explanation detailing the types of issues that arose. Senior management, in consultation with the Chief Compliance Officer, will then review the documentation and consider the risks associated with acceptance of identification evidence that falls outside these procedures, thereafter, providing the personnel with advice and guidance, as appropriate.

19.5. The risks considered in the assessment and decision process, and the conclusions reached should be properly documented within the customer KYC file, with appropriate sign-off by the individuals involved. Only Senior Management, in consultation with the Chief Compliance Officer, may determine the High-risk level to be attributed to any customer or/ and approve documentation that does not meet the exact requirements of the Company's Anti-Money laundering policy.

19.6. All customers are subject to a risk assessment and risk ratings will be recorded in the file. Due diligence requirements must be commensurate with the risk level associated with the customer and enhanced due diligence will be necessary for all higher risk customers.

19.7. In addition to trigger-based reviews, Avantaa Gold Jewellery L.L.C shall conduct periodic review of Customer's KYC and conduct CDD based on the risk profile of the customer:

- High Risk Customers: Every 6 months
- Medium Risk Customers: Every 12 months
- Low Risk Customers: Every 18 months

19.8. In relation to customers who did not trigger an alert, Avantaa Gold Jewellery L.L.C may consider refreshing required information and conducting a simplified due diligence by asking the customer to confirm baseline information on file along with documentary proofs.

For customers who triggered an alert, a more in-depth assessment, and review of the customer activity, may be required.

20. Targeted Financial Sanction (TFS)

The United Nations Security Council (UNSC) can act to maintain or restore international peace and security under Chapter VII of the United Nations (UN) Charter by imposing sanctions measures under Article 41, encompassing a broad range of enforcement options that do not involve the use of armed force.

UNSC sanction regimes focus mainly on supporting the settlement of political conflicts, nuclear non-proliferation, and counter-terrorism. These regimes include measures ranging from comprehensive economic

and trade sanctions to more targeted measures, such as arms embargoes, travel bans, and restrictions on dealing with certain financial or commodity transactions.

The UAE, as a UN member (and a UNSC member in 2022-23), is mandated to implement UNSCRs, including those related to UN sanctions regimes. Consequently, through the Cabinet Resolution No. 74 of 2020, the UAE implements UNSCRs on the suppression and CTF, and countering the financing of proliferation of Weapons of mass destruction (CFP), including targeted financial sanctions (TFS).

The term 'targeted sanctions' means that such sanctions are against certain individuals, entities, groups, or undetakings.

The term 'TFS' includes both asset-freezing and prohibitions to prevent funds or other assets from being made available, directly, or indirectly, for the benefit of sanctioned individuals, entities, groups, or organizations.

The list of UN sanction regime measures includes freezing of funds and prohibition of fund and service provision, in accordance with UNSC resolutions. The sanctioned (listed) individuals, groups, or entities include:

1. Islamic State in Iraq and the Levant (Da'esh), Al-Qaida, and associated individuals, groups, undertakings and entities	Listed by the UNSC
2. The Taliban, and associated individuals, groups, undertakings and entities.	
3. Any Individual or entity included in the Local Terrorist List, according to UNSCR 1373 (2001)	Listed by the Cabinet of the UAE.

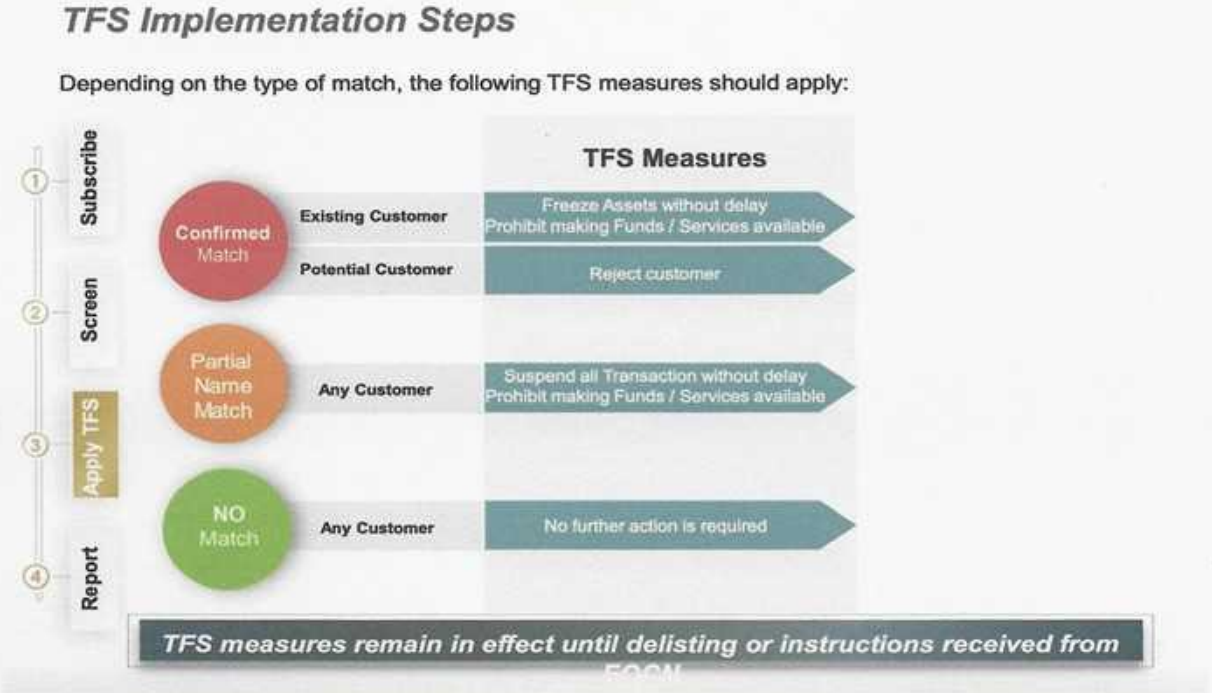
The Proliferation of weapons of mass destruction (WMD):

1. Democratic People's Republic of Korea (DPRK): nuclear-related, other weapons of mass destruction-related and ballistic missile-related programs.	Listed by the UNSC
2. Islamic Republic of Iran: nuclear programs.	

Other UN sanctions regimes with TFS

1. Somalia	Listed by the UNSC.
2. Iraq	
3. Democratic Republic of Congo (DRC)	
4. Related to the involvement of terrorist bombing in Beirut (2005) plus restrictive measures in relation to UNSCR 1701 (2006) on Lebanon.	
5. Libya	
6. Central African Republic (CAR)	
7. South Sudan	
8. Mali	
9. Yemen	

There are four main obligations on all persons, natural or legal in the UAE to implement Targeted Financial Sanctions (TFS)



20.1. Targeted Financial Sanction (TFS) Process

- We follow the strict adherence to the name screening on eachtransaction and ensure that no transaction is done with the customer's name that appear in any list (of known specially designated nationals (SDN) or suspected terrorists or terrorist organizations or any blacklist or posing risk of Proliferation Financing provided by the UAE Regulatory Authorities.
- WE ensures that the Name Screening is done on a regular and transactional basis, including on aliases names "aka", which means other known names
- WE have an automatic name screening system which can be automatically with screen the names of each customer and beneficiary against the sanctioned list every day.
- In the event that there is a possible match of a customer name with that of the blacklist, there is a provision to put the transaction on hold.
- The details of the name match on the SDN list are checked against details of the customer and beneficiary.
- In the event of an exact match i.e., it is determined that the name is on the blacklist or on TFS list, the transaction is withheld and immediately reported to the Financial Intelligence Unit & EOCN with FFR (Fund Freeze Report) and if Potential match is identified then the transaction is suspend and PNMR is reported via GoAML system to the regulatory authority, if any other matches on any other list STR/SAR is reported via GoAML system following the internal risk controls without tipping-off the customer.

- WE understand that the failure to report the same could result in fines, penalties, reputational and commercial loss.
- In the event the details of the customer do not match with the SDN list, the transaction and onboarding are released for further processing.
- The blacklists should be updated on a regular basis to avoid omission of names which may be recently added or deleted by the above-mentioned authorities.
- It is recommended to subscribe for alerts from OFAC, UN, EU, and other relevant paid sources.
- WE maintain its internal watch list for addition and deletion of the persons with whom the company does not want to deal with according to the risk he/she may expose the company to any risk, also conduct searches on google to check adverse or negative news on its customers as a part of its EDD process and take due senior management approval in such cases.
- Any name screening that Identifies as PEP or on sanctioned list is escalated for the approval of the owner with the detailed EDD on the customer.

The Logs related to the screening of the transactions should be kept for 5 years from the date of transaction for records

Procedure to cancel or lift the freezing measures:

The procedure for cancellation of Freezing and any other TFS measures taken against an individual, group or entity with a name identical or similar to an individual, group or entity listed, or the person who has been adversely affected by the Freezing or any of the Other Measures due to be listed in the Local Terrorist List, is the following:

1. Submit a written application to the Executive Office accompanied with all supporting documents to the email: iec@uaeiec.gov.ae. o Follow the procedures and attach all supporting documents to substantiate your claim stated online at https://www.uaeiec.gov.ae/.
2. The Executive Office reviews the request and forwards it to the Supreme Council for National Security (Supreme Council) for its decision.
3. The Executive Office notifies the applicant and the relevant Supervisory Authority

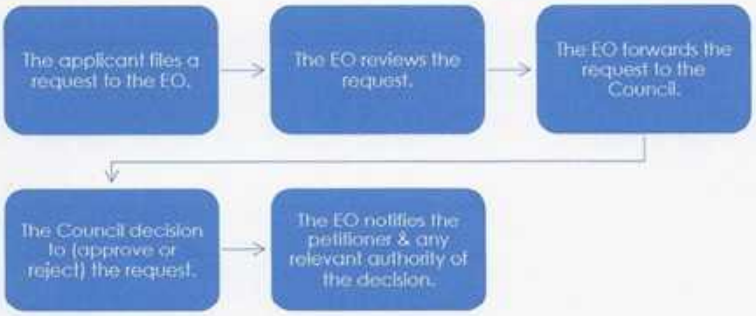


Exhibit 4: Procedure to request the cancellation of freezing and/or other TFS measures as designated by the Local Terrorism List

Grievances to the court:

If the application is rejected by the Supreme Council, or if no response to the application is received within 30 days from date of its submission, the applicant may file a grievance before the Competent Court within 60 days from the date of notification of the rejection, or after the response period has elapsed. The court's decision on the grievance may not be appealed, and if the court rules to reject the grievance, a new grievance may only be filed after 6 months from the date of rejection of the grievance, unless a serious reason that is accepted by the president of the Court arises before the expiry of such period.

21. Politically Exposed Person (PEP)

Avantaa Gold Jewellery L.L.C shall endeavour to establish and record the true and full identity of any FPEP/DPEP/HIO as well as their immediate family members and any related entities. Avantaa Gold Jewellery L.L.C has established policies and procedures to reduce the risks of FPEP/DPEP/HIO relationships by conducting EDD before either establishing a business relationship or continuing an existing business relationship where the customer or the beneficial owner is found subsequently to be a FPEP/DPEP/HIO.

FPEP is a Senior Official in the executive, legislative, administrative, military or judicial branches of a foreign government, their immediate family members and close associates. A DPEP is an individual residing in the UAE who also falls into one of the above-mentioned categories.

21.1. Definition of FPEP/DPEP/HIO

All senior political and government leaders and functionaries including:

- Heads of State, Presidents and Prime Ministers Government Ministers and Deputy Ministers;
- Political Party Leadership
- All Members of Parliament/Senate
- Key Senior Government Functionaries
- Judiciary
- Legislature
- Senior Military Officers
- Ambassadors
- Key leaders of state-owned enterprises
- Heads of government agencies
- Private companies, trusts or foundations owned or co-owned by FPEP/DPEP/HIO, whether directly or indirectly
- FPEP/DPEP/HIO family members can include close family members such as spouses, siblings, children, cousins and parents, and may include other relatives and relatives by marriage.
- Close associates may include personal advisors/consultants, colleagues or the FPEP/DPEP/HIO's fellow shareholders and any persons who could potentially benefit significantly from close business associations with the FPEP/DPEP/HIO.

21.2. EDD on FPEP/DPEP/HIO customers:

- Identify FPEP/DPEP/HIO through screening against watch lists and Identification documents.
- Obtaining a written approval from Avantaa Gold Jewellery L.L.C senior management for authorization on any potentially sensitive FPEP/DPEP/HIO relationships
- Taking reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of the funds
- Applying enhanced monitoring to the relationship in accordance with the risks identified

22. Sanctions Screening

22.1. Sanctions Policy

Avantaa Gold Jewellery L.L.C has adopted a global sanction policy and is fully committed to screening customers and transactions against lists of entities (natural or juridical) and/or countries issued by government/competent authorities, on a real-time basis. Avantaa Gold Jewellery L.L.C ensures to conduct its business in compliance with all laws applicable.

22.2. Sanction Screening Procedure

Screening is conducted prior to the customer onboarding. All the parties involved in the onboarding profile is screened against the relevant lists.

Avantaa Gold Jewellery L.L.C retains the services of Winnow Management Solutions Screening tool to conduct the sanctions screening. The major list covered are UAE, UNSC, PEP, OFAC, EU, UK, and many more lists are covered.

23. Monitoring Policy:

The transaction monitoring system clause specifically requires the institution to establish a system that can identify unusual or suspicious patterns of transactions, such as large or frequent cash transactions, and report them to the relevant govt. authorities.

The transaction monitoring system should be designed to unusual activities based on various criteria such as transaction amount. frequency. nature, location. or parties involved. It should also have appropriate controls, such as exception reporting and escalation procedures, to ensure that suspicious transactions are properly investigated and reported.

Overall, the transaction monitoring system is a critical component of an effective AML program, as it helps the entity to detect and to prevent money laundering and terrorist financing activities and comply with regulatory requirements.

The following methods are using by us to monitor the transactions of the customers.

1. Customer Base
▪ PEP,
▪ Complex Ownership
▪ Non-Resident
2. Transaction Base
▪ Large volume of cash transactions.

	▪ Interrelated transactions
	▪ Multiple transactions
3. Threshold Base	
	▪ Transactions crossed 55000AED and above
4. Location base	
	▪ Involvement of high-risk jurisdiction in either customer nationality, residency or countries of operations

24. Suspicious Activity Reports (SAR) / Suspicious Transaction Reports (STR)

(FATF Recommendation 20)

24.1. Identifying & Reporting of Suspicious Transactions

All employees of Avantaa Gold Jewellery L.L.C, the senior management and the Board of Directors are responsible for reporting any suspicious activity in accordance with these AML Policies and Procedures and the Standards.

A 'suspicious activity' is deemed to be where there are reasonable grounds to suspect that an individual or entity might be laundering money and/or assisting and/or financing terrorist activity. Avantaa Gold Jewellery L.L.C acknowledges that it is a vital part of our regulatory compliance obligation to report any suspicious transactions. Avantaa Gold Jewellery L.L.C is also aware that failure to report any such suspicion to the respective Financial Intelligence Units (FIUs) may result in financial penalties, imprisonment and irreparable reputational damage to those concerned and the organization as a whole.

CDD/EDD and ongoing monitoring provides the basis for recognizing unusual and suspicious transactions and events. Avantaa Gold Jewellery L.L.C has established CDD/EDD procedures and has monitoring systems in place to assist staff in effectively identifying any suspicious activity. Furthermore, Avantaa Gold Jewellery L.L.C provides AML & CFT training to all employees to better equip them in their daily AML & CFT routines, specifically in being able to recognize red flag behaviors that may indicate unusual and suspicious transactions.

Avantaa Gold Jewellery L.L.C commits to:

- provide AML & CFT training to its staff to ensure sufficient knowledge and guidance to enable them to form suspicion when ML/TF is taking place
- recognize that a transaction, or a series of transactions, is unusual and, from an examination of the unusual, whether there is a suspicion of ML/TF
- Enable staff to identify and assess the information that is relevant for judging whether a transaction or instruction is suspicious in the circumstances.

Avantaa Gold Jewellery L.L.C acknowledges the importance of the "time factor" in reporting suspicious transaction and therefore undertakes that reporting must be within a reasonable timeframe and with as much detail included as possible.

24.2. Internal Reporting Line and the STR On-line Reporting System

Step 1: Staff/Creator of SAR/STR forwards the report to the MLRO

Staff complete the details of their suspicion and signs the SAR/STR form enclosing supporting documentation.

Step 2: The MLRO will acknowledge the receipt of the SAR/STR form.

Step 3: The MLRO will acknowledge the receipt of SAR/STR. He/she will review and analyse the report; and if concurred, sign the SAR/STR and prepare a final report to FIU.

Step 4: SAR/STR is registered in the goaml portal with the supporting information and documentation.

Documentary evidence regarding all internal STRs, details of investigations undertaken and reasons are documented safely for future monitoring and record keeping.
Relationships with customers who are subject to SAR/STRs will be assessed on a risk-based approach.

25. Typologies & Red Flags Indicators

25.1. Typologies FIU Strategic Analysis Report

a. <u>Trade-based money laundering (TBML) by DPMS entities:</u>

The analysis indicates a pattern involving DPMS entities using TBML techniques. It was perceived that DPMS entities are established as a 'front' for laundering illegal proceeds generated by crime, using TBML methods such as false invoices, phantom shipments, and fictitious sales agreements/contracts. This pattern also indicates that DPMS are possibly exploited to transfer/move foreign illegal proceeds through the financial system in the country disguised as trade-based activities. Another risk factor noted during the analysis is the use of multiple DPMS entities (i.e., network) by means of 'corporate vehicles' to facilitate the 'layering' of funds basically by sending/receiving large wire transfers or remittances to/from multiple local or international counterparties, and then circulating the funds amongst domestic entities with no apparent justification for such proceeds or movement.

b. <u>Money laundering through 'foreign currency exchange' by DPMS entities:</u>

Within this emerging trend, DPMS entities have been found to instruct individuals (who might be employees, representatives, or external parties) to undertake 'foreign currency exchange' (FOREX) services on behalf of the entity without involving the name of the DPMS entity in such transactions. In attempting to conceal the actual source of cash, it was further observed that when the amount exchanged exceeds the threshold,20 another individual will continue with the transaction to avoid the detection and documentation requirements. Some individuals involved in this trend state that the source of funds is either that of 'salaries' or 'savings,' while the purpose is that of 'family maintenance' or 'travel.' The main currency involved was USD, followed by EUR and SAR respectively. In another scenario, the DPMS entity (under its name) conducts large FOREX transactions without justification or sufficient documentation to substantiate the volume of activity, as well as the source of cash. Aside from this, such entities have been found to be connected with a high value of cash imports and exports on a frequent basis. Moreover, the purpose of these transactions, as stated by

the entity, is either: (1) to pay suppliers who only accept cash as a payment method, or (2) to pay suppliers via cash in another jurisdiction (cross-border cash movement).

c. **Possible gold/cash smuggling via DPMS entities (conflict gold supply chain)**

DPMS entities are possibly involved in gold smuggling from conflict/affected and high-risk areas or in the illegal transport of gold through other high-risk jurisdictions. From there, gold enters the country and is further sold to other local DPMS entities, or is processed and re-exported to European countries.

This pattern is also linked to 'cash smuggling,' with 'cash' being noted as the main mode of transactions conducted by the same DPMS entities. Another factor observed is the involvement of multiple individuals in importing and exporting (mainly) cash on behalf of DPMS entities. TBML methods were observed to be correlated with this pattern, including the ownership structure of the DPMS entities involved, which was found to be 'complex' in some of the reviewed reports indicating the possibility of such entities hiding their true 'ownership'/UBOs. Moreover, there are indications that local associated refineries are sourcing gold from miners without conducting adequate 'customer due diligence' (CDD).

25.2. Red Flags Indicators

Red Flags are those behaviours or characteristics of the business transactions carried out with customers that might help us detect a Suspicious Transaction of money laundering and/or terrorist financing.

Red Flags show us certain behaviours of the customers and unusual situations during a transaction that might be an attempt to conceal money laundering activities. It must also be noted that not all transactions that present unusual or atypical behaviours are illegal activities. An "unusual" transaction might, after being carefully evaluated, show that the customer IS conducting perfectly legal operations.

In order to determine what is unusual about a transaction, It IS necessary to understand its complexity, amount, design, reiteration, if it serves no evident financial, business, or legal purpose. based on the characteristics and business-financial profile of the customer

In summary, there could be many elements that make a transaction suspicious. but in Order to evaluate it and prevent from reaching that status, it is Of It most importance the Comprehensive knowledge the Institution has of its customer, and the information the customer can submit to explain and validate the origin and purpose of such transaction.

Cash Transactions

1. Measures should be taken if client carrying out occasional transactions in favour of customer for amounts equal to or exceeding AED55.000 regardless if it is carried Out in single or several times.
2. Measures should be taken if client carrying out occasional transactions in form of wire transfer for amounts equal 10 or exceeding AED 3,500. Third Party cash transactions must be avoided.

General Transactions

1. Company representatives that avoid direct contact with our Company
2. Customers who frequently make payments routed through funds from so called "tax havens" or from countries that are considered non-cooperative by FATF, or if they send large amounts of money to these countries on a regular basis.
3. When a company has different people with authorized signature but there is no apparent relationship between them (whether business or family ties). Special attention should be paid when these are offshore companies located in tax havens.

4. Customer located in a country where there is a reportedly high drug-trafficking activity or known connections to terrorist Organizations, or a country that is considered as non-cooperative to combat money laundering, or a country that is not compliant with international standards.
5. Legal person, foundation or association that might have ties to a terrorist organization and conducts transactions.
6. Customers that seem to be acting on behalf of a third party and do not want to reveal the Transactions with foreign Customers.
7. Electronic transfers that do not have sufficient data to trace back the transaction.
8. Payments where the sender or beneficiary is a foundation, association or other non-profit organization that cannot provide a valid explanation of the source of the funds.
9. The origin of the funds is not consistent with the declared activity stated in the Customer Profile.
10. Payments broken into smaller amounts of money that are clearly trying to avoid a sum of Limit mentioned in AML regulations.
11. Payments received that do not provide clear information about the sender or payee in order to identify such transaction. Transfers Of large amounts of money to or from abroad that are to be paid in cash.
12. International transactions to customers/accounts without having the necessary background on those transactions, or where the staled business activity of the customer does not explain such transaction.
13. Customers who send or receive payments on a regular basis and in large amounts including telegraphic transfers, to or from countries considered as "tax havens" or non— cooperative according to the FATF.
14. Any type of Operation in which the customer refuses to provide the standard information requested if they provide Limited information or fake or that it is hard to verity for the institution.
15. Transactions with locations suspected of money laundering activities.

Other Factors

1. Staff who show a sudden change in their lifestyle or refuse to take time off or leave.
2. Staff who use their personal address to receive documentation from Customers.
3. Staff show sudden and significant increase in their operations.
4. When dealing with PEPs. special attention should be paid to their transaction- making sure these are consistent with the activity stated and their customer profile.
5. If the Entities Suspect or have reasonable evidence to suspect of the existence of funds That have ties to terrorism, terrorist acts or terrorist organizations, they should immediately inform that Financial Information Unit. The UN Security Council Resolutions for the Suppression of the Financing of Terrorism will be considered when handling these matters.
6. Customers who make unsound use of the services of Company
7. Legal persons owned by individuals of the same Origin or with participation of individuals of the same origin from jurisdictions that are considered as non-cooperative.

Red Flag Indicators for PF

Indicators of Possible Proliferation Financing as mentioned in Annex 1 to the 2008 FATF Typologies Report on Proliferation Financing

(i) Transaction involves person or entity in foreign country of proliferation concern.

(ii) Transaction involves person or entity in foreign country of diversion concern.

(iii) The customer or counterparty or its address is similar to one of the parties found on publicly available lists of "denied persons" or has a history of export control contraventions.

(iv) Customer activity does not match business profile, or end-user information does not match end-user's business profile.

(v) A freight forwarding firm is listed as the product's final destination.

(vi) Order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user.

(vii) Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped, (e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry).

(viii)Transaction involves possible shell companies (e.g. companies do not have a high level of capitalisation or displays other shell company indicators).

(ix) Transaction demonstrates links between representatives of companies exchanging goods i.e. same owners or management.

(x) Circuitous route of shipment (if available) and/or circuitous route of financial transaction.

(xi) Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws.

(xii) Transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.

(xiii)Transaction involves shipment of goods inconsistent with normal geographic trade patterns (e.g. does the country involved normally export/import good involved?).

(xiv)Transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws

Red Flag Indicators for TF

Customer's characteristics and associates

1. An account owner's name or counterparty is listed on a terrorist list (foreign or local).
2. A customer who is identified as a family member or relative to a designated person due to terrorism/TF concerns.
3. Politically Exposed Persons (PEPs) with links to conflict zones or extremist groups.
4. Customer associations with entities suspected of trading in conflict gold or individuals from high-risk jurisdictions linked to gold smuggling in conflict zones.
5. A customer is dealing with a counterparty who is a subject of a previously filed STR/SAR concerning possible TF activities. 6. A customer is dealing with a counterparty who is the subject of adverse news concerning possible TF activities.
7. Customer's counterparties are reported or observed to have similar suspicions in relation to terrorism or TF.

Transactions involving high-value items

- A business account conducts a high volume of transactions periodically in specific commodities that are not in line with the customer's business. These commodities could be traded for cash or shipped to areas of conflict (e.g., used or new cars).

- A customer (owner, authorizer of the account, etc.) from countries known to support terrorist activities and organizations conducting trade activities in gold or transactions with trade parties located in areas of conflict known for illegal mining/conflict gold
- A personal account receiving a high value of fund(s) as a salary from non-financial businesses and professions (e.g., accountant, lawyer) abroad, while the customer is known to the reporting entity to be an owner of a high-value industry business (e.g., gold, diamonds, oil, electronics).
- Multiple companies trading in precious metals and stones owned by the same owner/frequent owners from a country known for being home to an identified terrorist group.

26. Exit Policy

Exiting the Relationship/Blocking of Customers
Where Avantaa Gold Jewellery L.L.C does not believe that it can effectively manage the money-laundering risk associated with a business relationship, it will not enter into or maintain that business relationship.

Customers identified to pose high risk even once all the mitigating measures are taken into account, are subjected to blocking from making any further transactions upon instructions from the MLRO.

27. Tipping-Off and Confidentiality

(FATF Recommendation 21)
It is an offence ("Tipping Off") to reveal to any person any information, which might prejudice an investigation; if a customer is told that a report has been made, this would prejudice the investigation and an offence would be committed. It is Avantaa Gold Jewellery L.L.C's policy to prevent any directors, officers and employees committing the offence of tipping off.

Companies, their directors, officers and employees should be:

(a) protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred; and

(b) prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU. These provisions are not intended to inhibit information sharing under Recommendation 18.

In the conduct of KYC, queries may include asking the customer questions, based on common sense, which a reasonable person would ask in the circumstances. Such enquiries, when conducted properly and in good faith, do not constitute tipping off.

In case of any suspicion, staff should not directly refuse a transaction or onboarding of a customer in direct words, since the suspicion could be wrong; the customer may have all the necessary valid supporting details and/or documents had staff conducted an enhanced due diligence exercise. Any refusal could be deemed as "Tipping Off" which is an offence.

When exiting a business relationship, care should be taken not to Tip Off the customer and the MLRO should always be consulted in such circumstances where it is necessary to exit or not enter into a business relationship with a customer.

28. Employee Screening and Monitoring

All new employees are screened against watch lists upon acceptance of an offer letter and notified to the Compliance & AML function.

Should any negative findings appear on a search, the MLRO and HR will have decision making powers as to what action is taken in relation to such findings, based on the nature of the findings and a risk-based approach.

29. AML & CFT Compliance Independent Review

To ensure the effectiveness and sustainability Of an Anti-Money Laundering (ANIL) Compliance program, a comprehensive periodic review must be conducted to assess the adequacy of the program's policies, procedures, compliance officers' functions, and other control.

This independent review aims to evaluate and test whether the policies, procedures, and controls align with regulatory guidelines and provide recommendations for changes and modifications to enhance the program's effectiveness in combating money laundering and terrorism financing.

Guidelines

Internal and external audits are crucial in assessing the procedures of our company.

An External Audit refers to the assessment of a company's internal procedures by an independent party who is not affiliated with the organization. To ensure the credibility and accuracy of the audit findings and conclusions, the auditors must possess sufficient qualifications. [t is recommended that an external audit be conducted annually by an independent audit firm.

Internal Audit may be conducted by an organization's internal audit department or outsourced to capable partners. To ensure the effectiveness of internal audits, a well- defined audit program and checklist should be in place. It is recommended that such audits be conducted every six months. The auditor should report their findings directly to the owner.

Scope of Independent audit work:

The following are key areas that must be examined to evaluate the adequacy Of the Customer Due Diligence (COD) policies, procedures, and processes, and ensure compliance with internal requirements.

- Review the policies, procedures, and processes for COD and assess their compliance with applicable laws and regulations.
- Conduct appropriate transaction testing, with a particular focus on high-risk operations (products, services, customers, and geographic locations) on a sample testing basis.
- Evaluate the training program, including its comprehensiveness, accuracy of materials, training schedule. and attendance tracking.

- Review the integrity and accuracy of management information systems used in the AML compliance program, if any.
- Review the policies, procedures, and processes for suspicious activity monitoring and assess their effectiveness for generating reports, screening blacklists, flagging unusual transactions, and more.
- Evaluate the Suspicious Transaction Reporting (STR) systems, including the research and referral of unusual transactions. Testing should include a review of policies. procedures, and processes for referring unusual or suspicious activity from all business lines to the personnel or department responsible for evaluating unusual activity.

30. Training

30.1. We believe that creating a compliance and control culture among its employees is the best tool to Combat money laundering. Therefore, there's an ongoing effort to promote staff training, development and awareness programs around the many aspects that comprise the laundering of criminal proceeds and terrorist financing.

30.2. In order for their ML/FT risk assessment and AML/CFT mitigation measures to be effective, we should ensure that their employees have a clear understanding of the ML/TF/PF risks that is exposed to and can exercise sound judgment, both when adhering to the company's AML/CFT risk mitigation measures and when identifying suspicious transactions. Furthermore, due to the ever-evolving nature of ML/TF/PF risks, we should ensure that their employees are kept up to date on an ongoing basis in relation to emerging ML/FT typologies and new internal and external risks

30.3. We shall provide education and training for all its staff and personnel, including directors and officers, to ensure that they are fully aware of their personal obligations and responsibilities in combating money laundering and financing of terrorism and illegal organization, and so that they are familiar the system in place for reporting and investigating suspicious matters.

30.4. We shall, conduct induction training to the new staff within 30days of their joining, make arrangements for refresher training to remind existing key staff and officers of their AML/CFT responsibilities and to make them aware of any changes in the laws, national and international, and rules relating to AML/CFT yearly once.

30.5. We should also screen staff to ensure high standards when hiring employees. Effective screening and selection methods in relation the AML/CFT cultural compatibility of their employment candidates.

31. Statutory Reporting

We must inform the Financial Intelligence Unit (UAE) about following:

Transactions as per Ministry of Economy (UAE) circular dated 2nd June, 2021

- **Transactions with resident individuals**: Obtain identification documents (Emirates ID or Passport) for cash transactions equal to or exceeding AED 55,000 and register the information in the Financial Intelligence Unit's C'FIU") Go AML platform using the recently created 'Dealers in Precious Metals and Stones Report' (DPMSR).
- **Transactions with non-resident individuals**: Obtain identification documents (ID Or Passport) for cash transactions equal to or exceeding AED 55,000 and register the information in the FIU's Go AML platform using the newly created DPMSR,

- **Transactions with entities/companies**: Obtain a copy of the trade license, and identification documents (Emirates ID or passport) Of the person representing the company, in transactions equal to or exceeding AED55,000 in cash or through wire transfer. and register the information in the FIt-I's GO AML using the newly created DPMSR.

32. Record Keeping

(FATF Recommendation No. 11)

As a matter of record keeping policy, Avantaa Gold Jewellery L.L.C ensures that all customer and transactional information is kept confidential at all times; information should only be made available to authorized persons on a "need to know" basis. It is necessary to maintain an audit trail and hence the records/documents are available for presentation when required by the regulatory authorities, internal or external auditors or the Compliance& AML Department. The records are kept in corresponding computerized form. All records –are stored securely for easy retrieval.

Following the AML regulations outlined by the supervisory body, the ID, transaction record and other supporting details/documents are maintained on file for a minimum period of five (5) years from date of the last transaction with the customer. The only exception to the 5-year policy, is in relation to a legal case, in which case any records will be kept separately and may be retained beyond the five (5) year retention period until it is confirmed in writing that the case has been resolved or terminated by the court. All records are to be compiled simultaneously with the event, or as soon as possible thereafter.

Records to be kept include:

- All the customer transactions
- All attached supporting details/documents
- Counterparty identification documentations
- Records of all electronic payments and messages
- Records of SAR/STRs filed
- Employee Training Records
- KYC records

33. AML/CFT Administrative Violations and Penalties

As per Federal Decree – Law (20) of 2018;

The Regulator has the authority to impose the following administrative penalties on the financial institutions, designated nonfinancial businesses and professions and non-profit organizations in case they violate the present Decree-Law and its Implementing Regulation:

a. Warning.
b. Fines of no less than AED 50,000 (fifty thousand dirham) and not more than AED 5,000,000 (fivemillion dirham) for each violation.
c. Banning the violator from working in the sector related to the violation for the period determined by the regulatory authority.
d. Constraining the powers of the Board members, supervisory or executive management members,managers or owners who are proven to be responsible of the violation including the appointmentof temporary inspector.

e. Arresting Managers, board members and supervisory and executive management members whoare proven to be responsible of the violation for a period to be determined by the Supervisory Authority or request their removal.
f. Arrest or restrict the activity or the profession for a period to be determined by the supervisoryauthority.
g. Cancel the License.

In all the cases, the Regulatory Authority shall publish the administrative penalties through variousmeans of publication from time to time.

No.	Applicable Article in the Implementing Regulation	Violation	Administrative Fine (AED)
1	Article (4) Clause 1	Failure to undertake the actions and procedures necessary to identify the risks associated with the crime in the violator's field of work.	100,000 AED
2	Article (23)	Failure to identify and assess the risks that may arise in the violator's field of work when developing the services that the violator offers or when conducting new professional practices through its facility.	100,000 AED
3	Article (4) Clause 2	Failure to undertake the actions and procedures necessary to mitigate the risks identified based on the results of the National Risk Assessment or the Self- assessment process given the nature and scale of the violator's business.	50,000 AED
4	Article (20)	Failure to implement internal policies, procedures and controls within the facility aimed at combating crime or preventing involvement in suspicious business relationships.	50,000 AED
5	Article (4) Clause 2/B + Article (22) Clause 1	Failure to take the necessary enhanced due diligence measures to manage high risks.	200,000 AED
6	Article (4) Clause 3	Failure to take the necessary simplified due diligence measures to manage low risks.	50,000 AED
7	Article (5)	Failure to undertake the necessary customer due diligence measures before establishing the business relationship or resuming a business relationship or performing a transaction under the customer's name or in his/her favor.	100,000 AED
8	Article (8) Clause 3	Failure to undertake the necessary measures to understand the purpose of the business relationship and its nature, or the failure to acquire any information pertaining to this purpose when needed.	50,000 AED
9	Article (8) Clause 4	Failure to undertake the necessary measures to understand the nature of the customer's business, the ownership structure of his/her business, and the extent to which the customer has control over that business.	50,000 AED

10	Article (8) Clause 1 and 2	Failure to verify the identity of the customer and the real beneficiary or their representative using documents or data collected from reliable and independent sources before or while establishing a business relationship or opening an account or prior to performing a transaction for a customer with whom no business relationship has been established.	100,000 AED
11	Article (7)	Failure to undertake the due diligence measures pertaining to the ongoing supervision of customers while conducting the business relationship.	50,000 AED
12	Article (13)	Failure to notify the Financial Intelligence Unit of the suspicious transaction report when the customer due diligence measures were not taken before establishing or continuing a business relationship with the customer or performing a transaction for the customer or under his/her name.	200,000 AED
13	Article (17) Clause 1/A	Delay in notifying the Financial Intelligence Unit of the suspicious transaction report in case there is suspicion or if there are reasonable grounds to suspect that the business relationship with the customer is in whole or in part linked to the crime, or that the customer's funds that are subject to the business relationship are in fact proceeds of a crime or were used in committing a crime.	100,000 AED
14	Article (17) Clause 1/A	Failure to provide the Financial Intelligence Unit with the additional information it requires regarding the matter reported in the suspicious transaction report.	200,000 AED
15	Article (14) Clause 1	Dealing with shell banks in any way.	1,000,000 AED
16	Article (14) Clause 2	Opening or maintaining bank accounts using pseudonyms, fictitious names or numbered accounts without the account holder's name.	1,000,000 AED
17	Article (15)	Failure to conduct due diligence measures on politically exposed persons before establishing or continuing a business relationship with such customers.	100,000 AED
18	Article (18) Clause 1	Disclosing, directly or indirectly, to the customer or any other person(s) that they have reported or are intending to report a suspicious transaction.	200,000 AED
19	Article (21)	Failure to appoint a compliance officer	50,000 AED
20	Article (19)	Failure to implement the measures prescribed by the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organizations with respect to customers from high-risk countries.	200,000 AED
21	Article (24) Clause 1	Failure to create records for keeping track of financial transactions with customers.	100,000 AED
22	Article (24) Clause 3	Failure to create records that keep track of financial transactions with the customers in an organized manner, which prevents data analysis and tracking of financial transactions.	50,000 AED

23	Article (24) Clause 2	Failure to keep records and documents related to the financial transactions for a period of five years from the date of concluding the transaction or terminating the business relationship with the customer, or from the date of completion of the inspection of the customer's facilities.	50,000 AED
24	Article (24) Clause 4	Failure to make all the information pertaining to the customer due diligence, ongoing supervision, and the results of their analysis, records, files, documents, correspondence and forms available to the competent authorities upon request.	50,000 AED
25	Article (21) Clause 4	Failure to provide training for the facility's employees on combating money laundering and the financing of terrorism.	50,000 AED
26	Article (60)	Failure to take the necessary measures regarding customers included in the international or domestic sanctions lists before establishing or continuing a business relationship with those customers.	1,000,000 AED

34. High-Risk Jurisdictions:

The following countries are in the grey list as mentioned by FATF as on 13th Jun 2025.

Algeria, Angola, Bolivia, Bulgaria, Burkina Faso, Cameroon, Côte d'Ivoire, Democratic Republic of the Congo, Haiti, Kenya, Lao PDR, Lebanon, Monaco, Mozambique, Namibia, Nepal, Nigeria, South Africa, South Sudan, Syria, Venezuela, Vietnam, Virgin Islands (UK), Yemen.

Newly added countries in Jun'25

Bolivia

Virgin Islands (UK)

NO LONGER SUBJECT TO FATF INCREASED MONITORING from 13th June'25

Croatia, Mali, Tanzania,

High-Risk Jurisdictions subject to a Call for Action

This blacklist country list is as follows:

- **Democratic People's Republic of Korea**
- **Iran**
- **Myanmar**

While engaging the business relationship with such blacklist and grey list customers, we adhered the strict policy of following EDD measures, ensure to collect the proper valid documents such as the customer ID, address proof, source of funds/wealth documents, adverse check, sanction check and most importantly we will take our senior management approval for establish the relationship with those countries resident and non-resident individuals and entities.

End of the Document