

AGORA PRIME METALS TRADING FZCO

Unit C2, DMCC Business Centre, Level 13, AG Tower
Dubai Multi Commodities Centre Authority (DMCCA), United Arab Emirates

Anti-Money Laundering, Counter-Terrorist Financing, Counter-Proliferation Financing and Sanctions Statement

Precious Metals and Precious Stones Business

Our Commitment

Agora Prime Metals Trading FZCO ("Agora Prime" or "the Company") is an international metals trading company headquartered in Dubai, United Arab Emirates. We trade precious metals, including gold and palladium, across Europe, Africa, Asia and the Middle East, and we are licensed by the Dubai Multi Commodities Centre Authority.

Precious metals are portable, liquid and valuable. Those same qualities make our sector attractive to those seeking to launder criminal proceeds, finance terrorism, finance the proliferation of weapons of mass destruction, or evade international sanctions. Agora Prime does not accept that risk as a cost of doing business. Our Board of Directors and senior management undertake that the Company will not allow its business, its accounts or its supply chain to be used for any of these purposes.

This commitment is not aspirational. It is implemented through a documented compliance framework, a Board-appointed Compliance Officer with direct access to the Chief Executive Officer and the Board, and controls that apply to every client, counterparty, supplier and transaction without exception.

Who This Applies To

This statement governs the whole of the Company and its operations in relation to its precious metals business. It binds our Board of Directors, Chief Executive Officer, senior management and every employee, and it sets out the principles we apply when dealing with our external stakeholders.

- Clients — buyers, sellers, consignors, consignees, brokers and sub-brokers, authorised signatories, attorneys and the senior officers of corporate clients
- Suppliers and other participants in our supply chain
- Intermediaries, vessel owners, banks, insurers and financing institutions
- Any other counterparty to a transaction in which the Company takes part

Where a counterparty is unwilling to meet the standards described here, we do not proceed with the relationship.

Our Regulatory Framework

Because the Company holds a licensed precious metals activity, it is regulated as a Dealer in Precious Metals and Stones and as a Designated Non-Financial Business and Profession. Our supervisory authority is the Ministry of Economy of the United Arab Emirates.

Our framework is built on the UAE federal anti-money laundering and counter-terrorist financing legislation and its implementing regulations, as amended from time to time, together with:

- Cabinet Decisions governing terrorism lists, the implementation of United Nations Security Council Resolutions, beneficial ownership procedures and the proliferation financing control list

- Ministry of Economy circulars and guidance for Designated Non-Financial Businesses and Professions, and the supplemental guidance issued for Dealers in Precious Metals and Stones
- National guidance on targeted financial sanctions and counter-proliferation financing
- The findings of the UAE National Risk Assessment, and the recommendations, guidance and typology reports of the Financial Action Task Force and MENAFATF

The framework is reviewed at least annually, and sooner where the law changes, where our risk profile changes, or where the Company alters its strategy or structure.

Governance and Accountability

Responsibility for compliance sits at the top of the Company and is not delegated away from it.

Board of Directors and Chief Executive Officer

The Board and the CEO approve the compliance and governance framework, the underlying policies, procedures and risk methodology, and the appointment of a qualified Compliance Officer. They ensure the compliance function is independent, adequately resourced and has unrestricted access to information. They approve the enterprise-wide risk assessment, review reports on the effectiveness of the compliance function, approve training plans and budgets, and personally approve the establishment or continuation of any relationship assessed as high risk or involving a politically exposed person.

The Compliance Officer

The Compliance Officer reports directly to the CEO with a right of access to the Board. The role owns the design, implementation and testing of our controls; screening and due diligence decisions; the review of alerts and investigations; and all regulatory reporting and correspondence with the supervisory authority, the Financial Intelligence Unit and the Executive Office for Control and Non-Proliferation.

Three Lines of Defence

Our business, accounts and finance teams form the first line of defence: they meet the client, collect and verify documentation, and are trained and empowered to escalate concerns. The Compliance Officer forms the second line, setting standards, monitoring first-line controls and assessing risk. An independent audit function forms the third line, testing whether the first two are working as intended. Feedback flows across all three so that control design keeps improving.

A Risk-Based Approach

We do not apply the same controls to every relationship. We identify, assess and understand the money laundering, terrorist financing, proliferation financing and sanctions risk we are exposed to, and we apply measures proportionate to that risk. Where risk is higher, our controls are more intensive and more frequent. Where it is demonstrably lower, simplified measures may apply.

Risk is assessed across the following dimensions:

- Client risk — the type of client, their ownership and control structure, and their conduct
- Geographic risk — country of residence, incorporation, operation and transaction routing
- Product risk — the metals traded and the characteristics of the trade
- Industry and occupation risk — the sector in which the client operates and the source of their wealth
- Delivery channel risk — whether the relationship is established face to face
- Transaction risk — the method and structure of payment and settlement

At the enterprise level, the Company performs an annual enterprise-wide risk assessment that maps inherent risk, evaluates the controls that mitigate it, identifies residual risk and sets an action plan to close gaps. The assessment is reviewed and approved by the CEO and the Board.

Knowing Our Clients

We open a relationship only when we know who we are dealing with, who ultimately owns and controls them, and where their funds come from. Know Your Client is not a one-off exercise at onboarding; it is a continuing obligation for the life of the relationship.

Our process runs through registration, identification and verification, and is applied at a depth determined by risk:

Simplified Due Diligence

Applied only where overall risk is assessed as low and the client falls within a narrowly defined category, such as a company listed on an exchange with adequate beneficial ownership disclosure requirements, or an entity wholly or partly owned by the UAE government.

Client Due Diligence

Our standard measure. We identify and verify the client and the legal entity, confirm the nature of its business and the purpose of the relationship, identify and verify beneficial owners and authorised representatives, obtain address and authority evidence, and screen all parties against applicable sanctions lists. Identification documents are sighted and verified against originals, in person or by live video, and certified by the employee who performs the check.

Enhanced Due Diligence

Applied wherever risk is assessed as high, where a client or supplier is a politically exposed person, or where red flag indicators are present — for example, an unusually complex ownership structure, a cash-intensive business, nominee or bearer shareholdings, or a connection to a jurisdiction with weak controls. Enhanced measures include establishing source of funds and source of wealth with documentary evidence, adverse media and open-source research, verification of shareholders and directors from reliable sources, independent corroboration of wealth for very high net worth individuals, external intelligence reports where public information is inadequate, closer and more frequent monitoring, and CEO approval before the relationship proceeds.

Beneficial Ownership

We identify the natural person who ultimately owns or controls 25% or more of the shares or voting rights of a corporate client, or who exercises control by other means. Where ownership is deliberately layered or obscured, we look through the structure and may set a lower identification threshold. Where no beneficial owner can be established, we treat the senior managing official as the beneficial owner — and we treat the difficulty itself as a risk indicator.

Third Parties and High-Risk Countries

Where the paying party differs from the client with no apparent connection, we establish and document the reason, identify and verify the third party, and obtain a declaration and valid authority before proceeding. Clients connected to high-risk jurisdictions are subject to enhanced due diligence before any transaction, and we do not transact with countries subject to a FATF call for action.

We do not rely on third parties to perform due diligence on our behalf.

Sanctions and Targeted Financial Sanctions

Agora Prime complies fully with targeted financial sanctions. We do not make funds, assets, goods or services available, directly or indirectly, to any designated person, entity or group.

- Every client, beneficial owner, authorised party and counterparty to a transaction is screened before onboarding, throughout the relationship, and for twelve months after it ends
- Screening is performed against the United Nations Security Council Consolidated List and the UAE Local Terrorist List, and we take account of designations made by other major sanctions authorities
- Screening is not subject to any transaction threshold — it is applied in every case regardless of value
- Our screening capability uses exact, fuzzy and phonetic matching so that true matches are not missed through spelling or transliteration differences
- The Compliance Officer is registered to receive designation notifications so that list changes are actioned without delay

Where a confirmed match is identified, we freeze without delay, prohibit the provision of any funds or services, and report to the authorities within the prescribed timeframe. Freezing measures remain in place until the person is de-listed or a competent authority directs otherwise. Where a potential match is identified, we suspend the transaction without delay, report it and hold the suspension until we receive instructions. Screening records, including the resolution of false positives, are documented and available to the competent authorities on request.

We are alert to evasion as well as to designation. Renaming, front companies, unnecessary intermediaries and alternative payment networks are treated as red flags. The Company will not withhold, alter or omit information about a client or a transaction, will not accept knowingly incomplete or false identifiers, and will not provide misleading information to a counterparty or an authority.

Politically Exposed Persons

Politically exposed persons, their family members and their close associates are screened and classified at the due diligence stage, before any relationship begins. Where a client is identified as a politically exposed person, both the Compliance Officer and the CEO must approve the relationship and its continuation, source of wealth and source of funds must be established and corroborated, and the relationship is reviewed at least annually. We treat a person as politically exposed on the basis of their position, influence and exposure to corruption risk, not merely on the basis of a system result.

Counter-Proliferation Financing

Proliferation financing is the provision of funds or financial services used, in whole or in part, for the manufacture, acquisition, development, export, transfer, stockpiling or use of nuclear, chemical or biological weapons, their means of delivery and related materials, including dual-use goods diverted to illegitimate purposes.

We assess proliferation financing risk in terms of threat, vulnerability and consequence, and we apply particular scrutiny to any dealing with or connected to jurisdictions and networks associated with proliferation programmes, which characteristically rely on front and shell companies to disguise their activity. Our employees are trained to recognise dual-use goods and the control list categories published by the Executive Office for Control and Non-Proliferation, and to escalate any transaction that raises a proliferation concern before it proceeds.

Relationships We Will Not Accept

There are relationships the Company will not enter into, and will exit if they arise:

- Any client whose due diligence cannot be completed, or whose risk falls outside the Company's risk appetite
- Anonymous accounts, or accounts in fictitious names, numbers or codes
- Any person or entity appearing on an applicable sanctions list
- Shell banks and shell companies
- Clients who provide manipulated, forged or falsified documentation, or who refuse to provide the information we are required to hold

Where we decline or exit a relationship on suspicion of criminal conduct, we make no payment to the client or any beneficiary, retain the relevant records, and report to the Financial Intelligence Unit. Exit decisions are documented and, where required, the client and its officers are added to our internal watchlist.

Ongoing Monitoring

Due diligence at onboarding tells us who a client is. Monitoring tells us whether they are behaving as expected. The Company monitors client activity for the life of the relationship to confirm that transactions remain consistent with the client's profile, stated business and risk rating.

Every transaction is examined against five questions: who the client and beneficial owner are; what is being traded; where the transaction touches; why the client is transacting and whether it makes commercial sense; and for whose ultimate benefit it is being conducted. Transactions are also screened for sanctions exposure at a point at which they can still be stopped, including the parties, the intermediaries and financial institutions involved, and the payment references and stated purpose.

Alerts are reviewed to understand what triggered them, whether behaviour has changed, and whether the activity is consistent with the information we hold — seeking further information from the client where necessary, and without disclosing that an enquiry is under way. Due diligence records are refreshed on a risk-based cycle, and immediately where we discover contradictory information, a material change in ownership or structure, legal proceedings, adverse media, or unusual activity. High-risk relationships are reviewed most frequently.

Reporting to the Authorities

The Company reports to the UAE Financial Intelligence Unit and to its supervisory authority through the goAML platform, and cooperates fully with law enforcement and competent authorities, providing requested data and access to records.

- Suspicious transaction and suspicious activity reports are filed whenever the Compliance Officer has reasonable grounds to suspect that funds, a transaction or an attempted transaction are connected to a crime, regardless of amount
- Cash and qualifying wire transactions in our sector are reported through the dealer reporting regime within the prescribed timeframes
- Fund freeze and partial name match reports are filed where sanctions screening produces a confirmed or potential match

- Transactions involving persons or entities from jurisdictions subject to a call for action are reported before they are conducted
- Further information requested by the Financial Intelligence Unit is provided promptly and in full

Every employee has a direct, confidential channel to raise an internal suspicion with the Compliance Officer, who investigates it, documents the outcome and decides whether an external report is required. Decisions not to report are documented with reasons. Reporting is not discretionary and it is not deferred: suspicion is escalated without delay.

Our People

Controls are only as strong as the people applying them. Every employee — including directors, executive management and the Compliance Officer — is screened before appointment. Screening covers qualifications, employment history, police clearance and sanctions checks, and is repeated on an ongoing basis. Every employee signs an undertaking to comply with the applicable AML, CFT, CPF and sanctions requirements. Where screening identifies a designation, the individual is not appointed, and an existing employee's engagement is terminated and the matter reported.

All employees receive induction training within one month of joining and refresher training at least annually, tailored to their role. Training is assessed, and employees who do not meet the required standard are retrained. The programme covers the applicable law, our sector's specific risks and typologies, due diligence, sanctions and targeted financial sanctions, proliferation financing and dual-use goods, transaction monitoring, red flag indicators, reporting obligations and the prohibition on tipping off. Training records are maintained and retained.

Records

The Company maintains records in an organised and retrievable form so that a client relationship or a transaction can be reconstructed at the request of a competent authority at any time. Client identification and due diligence records, transaction records, source of funds evidence, risk assessments, monitoring and investigation files, reports made to the authorities and training records are retained for a minimum of five years from the end of the relationship, the date of the transaction, the date of the report or the closure of the case, as applicable, and longer where an investigation remains open.

Confidentiality and Protection for Those Who Report

Where a report has been made, or is being considered, our employees are prohibited from disclosing that fact — or any related information — to the client or to any other person. Tipping off is a criminal offence and a serious disciplinary matter.

Equally, no employee will be disadvantaged for raising a concern. Directors, officers and employees who report suspicion in good faith, or who freeze funds or decline to provide services in respect of a designated person, are protected from liability and will not face retaliation from the Company in any form.

Working With Us

Clients and counterparties should expect to be asked for identification and ownership documentation, for evidence of the source of funds behind a transaction, and for updated information during the course of the relationship. These requests are not a comment on any individual client. They are how a responsible metals trading business protects its counterparties, its banking relationships, its supply chain and the integrity of the market it operates in.

We would rather lose a transaction than compromise this framework.

Compliance enquiries

Questions about this statement, or requests for the compliance documentation required for counterparty onboarding, may be directed to the Compliance Officer at compliance@agoraprimetrading.com.