TROY

KIYMETLİ MADEN TİCARETİ A.Ş.
PRECIOUS METALS TRADE INC.

AML / CFT POLICY

ANTI-MONEY LAUNDERING ("AML"), COUNTERING THE FINANCING OF TERRORISM ("CFT") POLICY

x

INTRODUCTION

It is the policy of Troy Kıymetli Maden Ticareti A.Ş (Troy Precious Metals Tradings Inc.) to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the financing of terrorist or criminal activities. We will comply with all applicable requirements and regulations. Our AML/CFT policies, procedures and internal controls are designed to ensure compliance with all applicable regulations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

LEGAL FRAMEWORK

By enacting and issuing the Anti-Money Laundering Law 4208 in 1996 and several regulations and communiqués for implementation of that Law, Turkey has completed and adopted its legislative acts, regulations and financial system in compliance with the Forty Recommendations of FATF where it is enrolled. Purpose of the Law 4208 is to set down the principles applicable for prevention of money laundering, and to determine the assets that may be the subject of "money laundering" crime which is classified as a separate and independent offence in the Law.

In 1998, The Presidency of Financial Crime Investigation Board (MASAK) reporting to the Minister of Finance has been formed and established, and has been entrusted with the data collection, evaluation, implementation, audit, regulation and coordination tasks and functions relating to the legal obligations arising out of the Law 4208.

In 2006, new legislation of Turkey, Prevention of Laundering Proceeds of Crime Law, Law No: 5549, has been issued by Turkish FIU (MASAK). The purpose of this law is to determine the principles and procedures for prevention of laundering proceeds of crime. In addition, the new regulation regarding to the mentioned law has been issued in 2008 to explain the new methodology of client identification–verification, know your client principles, to determine the suspicious activities, corresponding banking, following customers' transactions, etc. With a view for strengthening the struggle against terrorism, and preventing laundering, and seizing, proceeds of crime derived from acts of terrorism, and developing international cooperation in the struggle against organized crime and terrorism, Turkey has ratified the agreements published by the United Nations, and is, in accordance with The Eight Special Recommendations of FATF.

CONTROLS PRIOR TO OPENING BASE / ACCOUNTS

Customers who want to open 'Metal and Currency Account' are checked in international warning lists (such as OFAC; UN Sanctions List, EU Black List). AML Officers use the following lists:

*OFAC SDN List (Office of Foreign Assets Control Specially Designated Nationals List), the list prepared by the Treasury of the USA.
http://www.treas.gov/offices/enforcement/ofac/sdn/sdnlist.txt

* EU Sanctions List, The warning list prepared by the European Union
http://ec.europa.eu/external_relations/cfsp/sanctions/list/version4/global/e_ct lview.htm

* Banned and sanctioned countries, the link for the details is
http://www.treas.gov/offices/enforcement/ofac/programs/

*Proscribed terror groups or organisations
https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2

*Financial sanctions: consolidated list of targets
https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets

US sanctions lists
https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx

UN sanctions lists
https://www.un.org/sc/suborg/

High risk jurisdictions lists

FATF high risk and non-cooperative jurisdictions list
http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)

Transparency International corruption perceptions index
http://www.transparency.org/research/cpi/overview

Transparency International corruption by territory
http://www.transparency.org/country

AML/CFT COMPLIENCE PERSON DESIGNATION AND DUITIES

We have a designated Money Laundering Reporting Officer ("MLRO"). The MLRO has full responsibility for our AML/CFT program. The duties of the MLRO will include monitoring our compliance with AML/CFT obligations, overseeing communication and training for employees and overseeing software modifications to ensure they comply with AML/CFT obligations. The MLRO will also ensure that we keep and maintain all of the required AML/CFT records The MLRO is vested with full responsibility and authority to enforce our AML/CFT program.

RISK-BASED APPROACH

By implementing a reasonably designed risk-based approach, TROY PRECIOUS METALS TRADING INC. identify the criteria to measure and mitigate potential money laundering and terrorist financing risks.
To assist the overall objective to prevent money laundering and terrorist financing through TROY, a risk-based approach; Troy determine the low risk clients, high risk clients, high risk products, service and transactions, all actions to be taken related this subjects, and pursuance policy related with monitoring activities.

A. LOW RISK LEVEL CLIENTS

1. Capital Markets brokerage companies and Portfolio management companies,
2. Banks,
3. Financing and Factoring companies,
4. Investments Trusts,
5. Investment Funds,
6. Depository Trust companies, in the frame of Capital Market Board regulation,
7. Financial Leasing companies,
8. Insurance, Reinsurance and pension companies,

B. HIGH RISK LEVEL CLIENTS

1. Country/Region Risks

It is prevailed, in case required regulations are not implemented and precautions are no taken to prevent money laundering of crime revenues or teror financing in the countries/regions where the clients are resident or linked in a sort of way.
Clients that are resident or linked with below mentioned countries/regions are taken into consideration as high risk client classification;

- Countries in FAFT list
- Countries which is Off-Shore Banking is active,
- Free Zones; Cross border centers,

- Tax heavens or countries as knows tax heaven
- Anti- democratic countries which is on the way of illegal drug trade, distributions, and the countries that corruptions, smuggling, terror rate is very high,

2. Client Risk

Clients are classified on risk based according to business activity in the frame of laundering crime revenues and terror financing, by considering legal regulation previsions.

Shell companies are determined as in high risk group and it is indicated that account will not be opened and even a single transaction will not be realized with that kind of companies.

C. HIGH RISK LEVEL PRODUCTS, SERVICE AND TRANSACTIONS

1. Cash Transactions

For our Individual and corporation clients we have limited their cash transactions as 5,000 TRY and all payments over that amount are realized through the banking system. However it is our principle to conduct KCY process for all our clients regardless the transaction limit.

We are conducting high amount cash shipments and payment transactions for the clients that meet all qualificaitons of our KCY process. All cash exports – imports are realized with declaration to Turkish Ministry of Custom and Trade.

Clients which business activity is banknote trading, or cash transactions or any business related with cash, are decomposed from Precious Metals companies and should be analyzed with this perspective, In terms of areas of usage and purpose of cash demand.

2. Electronic Transfers

Electronic transfers are the most risky transactions and therefore much more controls are needed. By taking into consideration the numbers of EFT, frequency, amount, previous periods averages and differences, periodically controls are conducted. Risk Analyze should be made considering EFT transaction realizes at which country/region as well as purpose of transfer.

3. Correspondent Transactions

For Precious Metals transactions, without making discrimination, we apply KYC process to all of our Clients and Correspondents. Also all official company documents are collected from the suppliers regardless opening account process. Our company working principles are parallel to that vision. We apply differentiated Due Diligence questionnaire to Precious Metals companies, Financial Instutions as well as Individuals.

For Electronic Money Transfers, we give priority to correspondents among the correspondents of our banks which have good references regarding concordance to international norms and regulations.

4. Precious Metals Buying –Selling Transactions against Security Deposit

Money laundering by the way of unpaid credits used against security deposits, is evaluated as risky transaction in banking and finance sector. These kind of risks are also in gold business since it is too open to manipulation. We conduct risk base approach for all transactions that is backed by security deposits.

5. Custody Transactions

Custody is also another risky service. So regardless the Client is corporational or individual it is our company to policy to complete all KYC process.

6. Complicated and Unusual Big Amount of transactions

In especially gold business, complicated and unusual big amount of transactions, products and services also carry high level of risk.

COMPANY POLICY AND ACTIONS TO BE TAKEN FOR HIGH RISK GROUP CLIENTS

In case of any transactions realized by above mentioned high risk group clients, or any request to realize transaction and benefit from TROY services without having account;

- Legal and Economic purpose of transactions must be known previously, and in case if doubts related with transaction, documents should be requested to back up the reality of transaction.
- Enhanced search must be done through the internet as well as public institutes.
- Regardless of the amount/quantity of transactions, as it is stated at document, identification mus be made and all needed documents should be provided.
- For high risk Clients and transactions, the source of fund should be searched by department authorized related with the purpose of transaction. In case the customer or transaction itself is found suspicions, it should be reported to MASAK immediately.
- In case any proof determined like information/document related with money laundering or terror financing, or if the authorized person convinced that there is serious evidence, Client instruction will not be executed and immediately will be reported to MASAK by department authorized. If transaction is realized, in that case suspicious transaction is reported to MASAK.
- Client identification does not mean just to get ID documents from Clients, also to ensure the truth and consistency of information of documents.
- Client's legal existence and company structure, name, title, authorized persons, company official documents, should be confirmed with the information is provided from public institutions, banks or other references.
- During the internal controls by AML compliance officer, in case any forgery, discrepancy is determined at presented documents, MASAK should be informed immediately.
- Jewellery companies, currency exchanges and its employees bank accounts should be monitored and ensured about identification of real beneficiary related with the mentioned transaction.
- For corporation clients, In case of instruction is not found in line with the profile of company's regular transaction and is found as suspicious, another confirmation should be taken from another authorized person or owner. This kind of transaction monitoring is very important and all employees should be warned and trained periodically.

PURSUANCE POLICY RELATED WITH MONITORING ACTIVITIES

- High risk group clients and transactions are monitored at every transaction through banking system, and instructions are realized by Troy after analyzing and getting final approval from Finance manager.
- Complicated and unusual high amount transactions are monitored and is taken action to ensure that there is not any problematical point, in case client representative still has doubts, immediately report to Compliance authorized as well as Manager.
- Requested transaction is been made cross check if it is in line with Client's profile, business activity, sources of funds etc.
- Dormant Accounts that is requested to be active for very high volume transactions, immediately is searched entirely to get more information and all collected info is reported to MASAK.
- In case one of an individual client's daily transaction request is recorded as 5 times bigger than 3 months total realized transactions, MASAK is reported immediately.
- In case fund transfer request for huge amount fund that is already dropped into Client's account 3 days before. Clients fund transfer request is examined as in the frame of purpose and direction. These kind of transactions must be under control of TROY and Client should be warned, further the account can be closed.
- Corporations and Individuals that is found on exclusion lists, are reported to MASAK after confirming mentioned Corporations and Individuals are in the blacks lists.

To assess that risk mitigation procedures and controls are working effectively, TROY internal AML/CTF procedures will need to be kept under regular review.

POLICY ON POLITICALLY EXPOSED PERSON

Definition

PEPs are individuals who are or have been entrusted with prominent public functions in a country, for example Heads of State or of Government, senior politicians, senior government, judicial or military officials. Senior executives of state owned corporations, important political party officials, business relationships with family members or close associates of PEPs involve reputation risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories. PEPs include the following:

- Current and Ex-Head & Deputy head of state or National Government (President, Prime Minister, Government Ministers, Provincial Governors, Cabinet Members their Deputies (assistants), Senior Ministerial staff, and Secretaries.
- Current and ex-Members of National and Provincial Assemblies and Senate.
- Senior Civil Servants including Senior Government Officials, Heads of Government Departments, Police Service etc • Senior Judicial & Military officials,
- Senior Executives of state-owned Corporations,
- Influential Religious leaders of National / International repute
- High ranking Officers in Diplomatic Service (Ambassadors, High Commissioners, Envoys, Attachés, Consul Generals, Consuls, Honorary Consuls, Counselors etc)
- Senior Political Party Officials and functionaries such as Leader, Chairman, Deputy leader, Secretary General, and Executive Committee or any other Senior ranks in party (does not include middle ranking or more junior individuals)
- Close family members of PEPs includes: Spouses, children, parents, siblings and may also include other blood relatives and relatives by marriage.
- Closely associated persons includes: Close business colleagues and personal Advisors/ Consultants to the politically exposed person as well as persons who are expected to benefit significantly by being close to such a person.

Relationships with PEPs shall be established with the prior approval of Head of Compliance.

Policy Rationale

PEPs and related individuals can pose unique reputation and other risks, in particular:

- Some corrupt PEPs around the globe have used traditional banking products and services as safe havens for misuse of funds, illegal activities and associated practices, including money laundering;
- PEPs enjoy prominence and are therefore under continuous public spotlight. Their financial affairs are highly magnified and could easily trigger adverse publicity and franchise risks for the Financial Institutions and also gold sector market players.
- There is a growing attention worldwide to the misuse of public funds and increased reaction against corruption at high government levels;
- There is increasing responsibility and liability for financial institutions, gold traders as well as banks and company personnel to undertake due diligence for establishing source of wealth and investigate fund flows of PEPs.

It is a Policy of the TROY;

- That relationships with PEPs should be established with the prior approval Head of Compliance with the advice of Managing Director.
- All such relationships should be classified under High Risk category.
- All Sanction Lists are controlled during EDD for Peps also
- Checking the customer's background through an internet search
- Consulting reports and databases released by various organizations that specialize in analyzing corruption risks.
- In case of a PEP is found in any sanction list, the account opening request is Rejected.

Risks Associated with PEPs

There is always a possibility, especially in countries where corruption is widespread, that such persons abuse their public powers for their own illicit enrichment through the receipt of bribes, embezzlement, etc.

Accepting and managing funds from corrupt PEPs will severely damage the bank's own reputation and can undermine public confidence in the ethical standards of an entire financial center. Since such cases usually receive extensive media attention and strong political reaction, even if the illegal origin of the assets is often difficult to prove. In addition, the company may be subject to costly information requests and seizure orders from law enforcement or judicial authorities (including international mutual assistance procedures in criminal matters) and could be liable to actions for damages by the state concerned or the victims of a regime. Under certain circumstances, the company and/or its officers and employees themselves can be exposed to charges of money laundering, if they know or should have known that the funds stemmed from corruption or other serious crimes.

Course of Action

All PEPs and their close associates or family member's accounts will be treated as High Risk Accounts and accordingly will need approval of Head of compliance. Head of compliance officer will accord approval on the recommendations of Manager. Furthermore, branch management must obtain additional information on the customer (occupation, volume of assets); intended nature of the business relationship; reasons for intended or performed transactions; additional information on the sources of funds or sources of wealth of the customer.
All High Risk Accounts will be subject to enhanced monitoring of business relations with the customer and annual reviews.

MONITORING OF TRANSACTIONS

The Company must pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. The Company must also have understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity in order to effectively control and reduce the risk. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should be noted and must be reported to the Corporate Office.

High-risk accounts have to be subjected to intensified monitoring. The Company should put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. The Company should ensure that a record of transactions in the accounts is preserved and maintained as required in terms of Prevention of Money Laundering Act (PML) Act, 1996. It may also be ensured that transactions of suspicious nature and/or any other type of transaction notified under (the law number 5549 article. 4 / caution code artc. 29) is reported to the appropriate law enforcement authority, within the stipulated time frame.

As part of monitoring and control activities, the Company procures that the personnel carrying out these activities have access to internal information resources. Monitoring and control activities include but are not limited to the following:

- Monitoring and controlling customers and transactions in the high risk group,
- Monitoring and controlling transactions conducted with risky countries,
- Monitoring and controlling complex and extraordinary transactions,
- Controlling, through sampling method, whether the transactions exceeding a predetermined limit are consistent with the customer profile,
- Monitoring and controlling linked transactions which, when handled together, are exceeding the limit requiring customer identification,
- Controlling completing and updating the information and documents about the customer which have to be kept in electronic media or in writing and the compulsory information which have to be included in electronic transfer messages,
- Monitoring whether a transaction conducted by the customer is consistent with the information about the customer's business, risk profile and fund resources on a permanent basis throughout the term of the business relationship;
- Risk-based control of newly introduced products and services which may be exposed to abuse due to technological developments.

MONITORING AND REPORTING OF UNUSUAL OR SUSPICIOUS TRANSACTIONS

TROY should pay attention to and properly document the background and purpose of all large, complex, and unusual transactions or patterns of transactions and insignificant but periodic transactions that have no apparent economic or visibly lawful purpose. A suspicious transaction is one that is inconsistent with a customer's known legitimate business or personal activities or with the normal business for that type of account. Suspicious transactions should be promptly reported to the Supervisory Authority. Where a suspicious transaction has been determined and there are reasonable grounds to believe that a money laundering offence has been or is about to be committed, customer representative should immediately inform all related departments. Employees of TROY are expected to cooperate fully with the law enforcement authorities and they shall not notify any person, other than a court, competent authority or other person authorized by law, that information has been requested by or furnished to a court by the Supervisory Authority. Employee(s) may be disciplined if they fail without reasonable excuse to report a potentially suspicious transaction. It is a criminal offence for anyone, following a disclosure to the Compliance Officer, to do or say anything that might either 'tip off' another person that a disclosure has been made or prejudice an investigation. It is TROY's policy to carry out appropriate money laundering checks on all clients (managed accounts or funds). The findings will be retained by the Compliance Officer.

ANTI FRAUD POLICY

This policy applies to any irregularity, or suspected irregularity, involving employees as well as shareholders, consultants, vendors, contractors, outside agencies doing business with employees of such agencies, and/or any other parties with a business relationship with TROY (also called the Company). Any investigative activity required will be conducted without regard to the suspected wrongdoer's length of service, position/title, or relationship to the Company.

Examples of Fraud and Fraudulent Behaviors:

- Usurpation of corporate interests for personal gain;
- Misappropriation of assets, embezzlement and theft;
- Payment or receipt of bribes, kickbacks or other inappropriate payments;
- Participation in sham or fraudulent transactions;
- Deceptive, misleading or false statements about corporate transactions
- Forgery or alteration of accounting record or vouchers;
- Failing to keep confidential trade secrets of the Company;
- Non-disclosure of material information needed for an informed investment decision; and
- Other fraud behaviors causing loss to the Company interests.

This is not an exhaustive list. If you are in doubt about the seriousness of your concern advice and guidance can be sought from the Internal Audit Department and the Audit Committee.

Reporting Fraud or Fraudulent Behavior

1) The Internal Audit Department shall establish and maintain reliable communications channels (telephone hotlines, e-mail and mail) allowing for the anonymous reporting of actual or suspected instances of fraud or fraudulent behavior committed by the Company or any of its employees, representatives or advisors. Contact information for the various channels of communication shall be publicized so that actual or suspected cases of fraud or fraudulent behavior and violation of business ethics can be reported.

2) Complaints and concerns relating to instances of actual or suspected instances of fraud or fraudulent behavior or questionable accounting, internal control or auditing matters shall be reportable through the established channels of communications and may be reported on an anonymous basis.

3) The Internal Audit Department shall promptly investigate alleged and/or reported instances of fraud or fraudulent behavior. If any member of the Company's senior management is involved in the alleged and/or reported instances of fraud or fraudulent behavior, a special investigation team shall be organized to conduct an investigation with the assistance of the Internal Audit Department and shall report directly to the Company's Board of Directors or a committee.

Quarterly reports shall be issued by the Internal Audit Department to the Board of Directors regarding the nature and status of any complaints and/or investigations involving fraud or fraudulent behavior. Such reports shall be retained and made available in accordance with the Company's customary document retention policies.

WHISTLEBLOWER POLICY

A whistleblower as defined by this policy is an employee of the company who reports an activity that he/she considers to be illegal or dishonest to one or more of the parties specified in this Policy. The whistleblower is not responsible for investigating the activity or for determining fault or corrective measures; appropriate management officials are charged with these responsibilities.

Examples of illegal or dishonest activities are violations of federal, state or local laws; billing for services not performed or for goods not delivered; and other fraudulent financial reporting.
If an employee has knowledge of or a concern of illegal or dishonest fraudulent activity, the employee is to contact his/her immediate supervisor or the Human Resources Director. The employee must exercise sound judgment to avoid baseless allegations. An employee who intentionally files a false report of wrongdoing will be subject to discipline up to and including termination.,

Whistleblower protections are provided in two important areas -- confidentiality and against retaliation. Insofar as possible, the confidentiality of the whistleblower will be maintained. However, identity may have to be disclosed to conduct a thorough investigation, to comply with the law and to provide accused individuals their legal rights of defense. The Company will not retaliate against a whistleblower. This includes, but is not limited to, protection from retaliation in the form of an adverse employment action such as termination, compensation decreases, or poor work assignments and threats of physical harm. Any whistleblower who believes he/she is being retaliated against must contact the Human Resources Director immediately. The right of a whistleblower for protection against retaliation does not include immunity for any personal wrongdoing that is alleged and investigated.

Record Keeping

To be compliant with AML/CFT Regulations issued by MASAK, shall maintain all necessary records on transactions, both domestic and international, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions) for a minimum period of ten years from completion of the transaction. The records shall be sufficient to permit reconstruction of individual transactions including the nature and date of the transaction, the type and amount of currency involved and the type and identifying number of any account involved in the transactions so as to provide, when necessary, evidence for prosecution of criminal activity. The transactions records may be maintained in paper or electronic form, provided it is admissible as evidence in a court of law. The records of identification data obtained through CDD process like copies of identification documents, account opening forms, CIF, verification documents and other documents along with records of account files and business correspondence, shall be maintained for a minimum period of ten years after the business relationship is ended. The identification records may be maintained in document as originals or copies subject to Troy's attestation. The company shall, however, retain those records for longer period where transactions, customers or accounts involve litigation or it is required by court or other competent authority. It must be ensured that TROY shall always be in a position to satisfy, on timely basis, any enquiry or order from the relevant competent authorities including law enforcement agencies and for supply of information and records as per law.