

ANTI-MONEY LAUNDERING - KNOW YOUR CLIENT POLICIES

1. INTRODUCTION

Inverteo ("Inverteo" or "the Company") aims to prohibit, detect and actively pursue the prevention of money laundering and terrorist financing activities. It is also committed to comply with all related laws, rules and regulations with full attention without engaging in any of the aforementioned illegal activities.

The Company's management is committed to compliance with Anti-Money Laundering ("AML"), Combating the Financing of Terrorism ("CFT") in accordance with applicable laws, and attaches extremely high importance to the disclosure of any money laundering schemes and/or terrorist financing activities.

Inverteo also requires its officers, employees, introducing brokers and affiliated companies to adhere to these standards to prevent the use of the company's products and services for money laundering and terrorist financing activities.

2. PURPOSE

The purpose of the "AML, CFT and KYC Policy", ("the Policy"), is to provide guidance on anti-money laundering ("AML"), counter-terrorist financing ("CFT") and Know Your Customer ("KYC"), which the Company follows to achieve full compliance with relevant AML and CTF legislation.

This policy applies to all Company officers, affiliated companies, as well as products and services offered by the Company. Any employee who fails to adhere to these policies and procedures will be subject to severe disciplinary action.

3. LEGAL FRAMEWORK

The Company is required to comply with the provisions of the applicable laws regarding the prevention of Money Laundering and Terrorist Financing. The main objective of these laws is to define and criminalize the laundering of proceeds generated by all serious crimes in order to deprive criminals of the proceeds of their crimes.

In accordance with the AML and CTF Laws, the Company is required to establish policies and procedures to prevent money laundering and Terrorist Financing activities.

The AML and CFT procedures, which are implemented by the Company, are based on the AML and CFT laws applicable in the United Mexican States, the recommendations of the Financial Action Task Force (FATF), in addition to other documents and information.

4. DEFINITIONS

4.1 - Money laundering

Money laundering is the process of creating the appearance that large amounts of money obtained from serious crimes, such as drug trafficking or terrorist activity, originated from a legitimate source.

There are three steps involved in the money laundering process: placement, layering and integration.

4.1.1 - Placement

Placement refers to the act of introducing "dirty money" (money obtained by illegitimate and criminal means).

4.1.2 - Stratification

Layering is the act of hiding the source of that money through a series of complex transactions and accounting gymnastics.

4.1.3 - Integration

Integration refers to the act of acquiring this money by supposedly legitimate means.

4.2 - Terrorist financing

Terrorist financing (proceeds of crime) is the process by which funds are provided for the financing or financial support of individual terrorists or terrorist groups.

A terrorist, or terrorist group, is one that has a purpose or activity to facilitate or carry out any terrorist action, and may involve: individuals or groups.

4.3 - AML / CTF

The term AML/CTF refers to "Anti-Money Laundering and Combating the Financing of Terrorism" or "Combating Money Laundering and Combating the Financing of Terrorism".

4.3.1 - Combating money laundering

Anti-Money Laundering ("AML") refers to a set of procedures, laws or regulations designed to stop the practice of generating income through illegal actions.

4.3.2 - Anti-Terrorist Financing

Counter Terrorism Financing ("CTF") refers to a set of procedures, laws or regulations designed to prevent the financing or provision of financial support to individual terrorists or terrorist groups.

4.4 - Financial Action Task Force (FATF)

The Financial Action Task Force on Money Laundering ("FATF"), also known by its French name, Groupe d'action financière (FATF), is an intergovernmental organization established in July 1989 by a summit of the Group of Seven (G-7) in Paris, initially to examine and develop measures to combat money laundering.

In October 2001, the FATF expanded its mandate to incorporate efforts to combat the financing of terrorism, in addition to money laundering.

The FATF's objectives are to set standards and promote the effective implementation of legal, regulatory and operational measures to combat money laundering, terrorist financing and other related threats to the integrity of the international financial system.

Beginning with its own members, the FATF monitors countries' progress in implementing the FATF Recommendations; reviews money laundering and terrorist financing techniques and countermeasures; and promotes the adoption and implementation of the FATF Recommendations worldwide.

The Working Group was charged with examining money laundering techniques and trends, reviewing actions that had already been taken at the national or international level, and establishing what measures still needed to be taken to combat money laundering.

In April 1990, less than a year after its creation, the FATF issued a report containing a set of Forty Recommendations, the objective of which was to provide a comprehensive plan of action needed to combat money laundering.

In 2001, the development of standards in the fight against terrorist financing was added to the FATF's mission.

In October 2004, the FATF published a Ninth Special Recommendation, further strengthening the agreed international standards for combating money laundering and terrorist financing: the 40 + 9 Recommendations.

In February 2012, the FATF completed a comprehensive review of its standards and published the revised FATF Recommendations. This revision aims to strengthen global safeguards and further protect the integrity of the financial system by providing governments with stronger tools to take action against financial crimes. They have been expanded to address new threats, such as the financing of the proliferation of weapons of mass destruction. The new standards also impose higher levels of transparency and stricter regulations to curb corruption. The 9 Special Recommendations on Terrorist Financing have been fully integrated with anti-money laundering measures. This has resulted in a stronger and clearer set of standards.

5. PROCEDURES

The provisions of the Laws adopted by the Company introduce procedures and processes that ensure compliance with the applicable Laws related to Money Laundering and Terrorist Financing activities.

5.1 - Customer categorization and identification procedures

The Company has adopted all the requirements of applicable laws regarding customer categorization and identification and due diligence procedures as explained below:

5.1.1 - Customer categorization

Customers are categorized according to their risk profile into three main categories as explained below:

a- Low risk customers.

The following types of customers are considered lower risk. It should be noted that the Company will collect sufficient information to establish whether the customer qualifies to be classified as a lower risk customer:

i- Credit or financial institutions located in another country that impose higher or equivalent requirements than those established by the Company's regulators.

ii- Listed companies whose securities are admitted to trading on a regulated market in other countries, which are subject to disclosure requirements compatible with EU legislation.

b- Normal risk customers

All clients that are neither High Risk nor Low Risk shall be considered Normal Risk Clients.

c- High Risk Clients

Clients with the following criteria are classified as High Risk due to the following conditions:

i- Non-face-to-face Clients.

ii- Client accounts in the name of a third person

iii- Accounts of politically exposed persons ("PEPs")

iv- Betting / electronic games through the Internet

v- Customers from countries that inadequately apply the FATF Recommendations

vi- Clients whose nature entails an increased risk of money laundering and terrorist financing

vii- Any other Client that the Company itself determines to be classified as such.

5.1.2 - Customer Identification (Due Diligence) a- Due Diligence Conditions

Customer Identification and Due Diligence procedures apply under the following conditions:

i- Establishment of a business relationship.

ii- There is a suspicion of money laundering or terrorist financing, regardless of the transaction amount.

iii- There are doubts about the adequacy of previously obtained customer identification data.

iv- The customer fails or refuses to provide the required data and information for identity verification and the creation of their economic profile, without proper justification.

b- Due Diligence Timing

i- Customer identification and due diligence must take place before establishing a business relationship or conducting a transaction.

ii- Customer identity verification may be completed during the establishment of a business relationship if necessary to avoid disrupting normal business operations and when there is a limited risk of money laundering or terrorist financing. In such a situation, these procedures must be completed as soon as possible.

iii- Existing records should be regularly reviewed to ensure that documents, data, or information remain up to date.

iv- The customer fails or refuses to provide the required data and information for identity verification and the creation of their economic profile, without proper justification.

v- When a customer account is opened, it should be closely monitored.

vi- Customer due diligence procedures will apply not only to all new customers but also to existing customers at appropriate times based on a risk-sensitive approach.

vii- At frequent intervals, the Company must compare the estimated turnover with the actual turnover of the account.

viii- Any serious deviations must be investigated, not only for potential action by the Company concerning the specific account in question but also to assess the reliability of the person or entity who referred the customer.

c- Due Diligence Procedures

The Company's practice for complying with legal requirements concerning customer identification follows a risk-based approach, detailed as follows:

i- Standard Customer Due Diligence Procedure

- Customer identification and identity verification based on information obtained from a reliable and independent source.

- For legal entities, take appropriate, risk-based measures to understand the customer's ownership and control structure.

- Obtain information on the purpose and intended nature of the business relationship.

- Continuously monitor the business relationship, including scrutinizing transactions during the course of the relationship to ensure that transactions are consistent with the data and information held by the firm concerning the customer.

ii- Simplified Due Diligence Procedure

Simplified procedures may apply to low-risk customers. These measures will be applied when there is no suspicion of money laundering, regardless of any waiver, exemption, or threshold, and not always when a business relationship is established.

iii- Enhanced Customer Due Diligence Procedure

The Company must apply enhanced customer due diligence measures in situations that, by their nature, may present a high risk of money laundering or terrorist financing.

The Company will take specific and appropriate measures to mitigate the high risk by applying one or more of the following measures:

- Ensure that the customer's identity is established through additional documents, data, or information.
- Apply supplementary measures to verify or certify the documents provided.
- Ensure that the first payment for transactions is made through an account opened in the customer's name. This account must be in a credit institution operating in a country that imposes requirements superior or equivalent to those set by the Company's regulators.

d- Verification Procedure

The Company will follow the verification procedure outlined below to verify the customer's identity during the establishment of a business relationship:

i- The Company will ensure that the construction of the economic profile, suitability assessment, and appropriateness assessment are conducted at all times before establishing a business relationship.

ii- Customers have a grace period of fifteen (15) days to provide the Company with their identification documents. During this 15-day period, the Company must ensure the following:

- The cumulative amount of funds deposited does not exceed USD 2,000.
- Funds can only come from a bank account or other means linked to a bank account in the customer's name.
- Notification/reminder emails will be sent to customers requesting their identification documents.
- Account closure in cases where the verification procedure is not completed after the grace period.
- The Company will not withhold any customer's funds, and accounts will not be frozen unless under suspicion of money laundering.

e- Other Due Diligence Matters

i- Politically Exposed Persons

Politically Exposed Persons ("PEPs") are individuals entrusted with prominent public functions in a foreign country, as well as those closely related to politically exposed persons.

The Company must adopt the following additional due diligence measures to determine whether a potential customer is a politically exposed person:

- Special approval from Senior Management prior to establishing a business relationship with the customer.
- Take appropriate measures to establish the origin of the customer's assets and the source of the funds related to the establishment of the business relationship or transaction.
- Perform enhanced and continuous monitoring of the business relationship.

ii- Anonymous or Numbered Accounts

The Company is prohibited from maintaining anonymous or numbered accounts. Additionally, the Company must pay special attention to any threat of money laundering or terrorist financing that may arise from products or transactions favoring anonymity. The Company will also take the necessary measures to prevent their use for money laundering or terrorist financing purposes.

iii- Performance of Due Diligence by Third Parties

The Company is authorized and may rely on third parties to meet customer due diligence requirements. However, in such cases, the ultimate responsibility for complying with these requirements remains with the Company, which relies on the aforementioned parties.

5.2 - Customer Account Opening Procedures and KYC Documentation

Before accepting new customers, the company will require these customers to provide certain information and identification documents.

5.2.1 - Account opening

a- Information required for account opening

All clients interested in opening an account with the Company are requested to provide certain information, which includes:

- i- Client's personal data
- ii- Construction of the client's economic profile
- iii- Evaluation of suitability / suitability of the client.

It is obvious that the identification of the client, including the construction of the economic profile and the suitability/suitability assessment, will be carried out prior to the establishment of the business relationship with the client.

b- Account opening procedure

- i- The client completes the account opening forms by filling in all the required information.
- ii- The responsible administrator collects all initial information from the client and sends it directly to Senior Management, as well as to the Anti-Money Laundering Compliance Officer for review, revision and approval.
- iii- After approval, the administrator records all necessary information in the Company's software systems and communicates it to related departments.

5.2.2 - KYC Documentation

Before accepting new customers and allowing them to trade with the Company, the following documents must be obtained for customer identity verification:

The identification documents required from natural persons (individual customers) to efficiently implement the Company's KYC procedures are as follows:

i- Proof of identity.

A valid government-issued proof of identity (passport, national ID card, driver's license, ...) which must include the customer's full name, the customer's date of birth, the customer's photograph and the validity status (expiration date and/or date of issue + Validity Period). It is also **INDISPENSABLE** for the client to take a photograph of him/her with his/her face, also known as a selfie.

ii- Proof of Residence/Domicile

A recent proof of address in the person's name (bank statement, utility bills, telephone bills, ...) which must include the client's full name, the client's home address and the date of issue (must not be more than 6 months old).

b- Legal Entities

A different identification procedure is followed for Legal Entities (corporate clients) interested in opening an account with the Company. These documentation requirements are presented below:

i- Incorporation documents

The form and name of the corporate documents may vary depending on the country of incorporation and/or the legal form of the company. However, the required government-issued corporate documents must include the name of the corporation, date and place of incorporation, registered office address, directors and authorized signatories, ownership structure/shareholding (names of shareholders and percentage of ownership), registered corporate activities.

These documents may include, but are not limited to, certificate of incorporation or certificate of registration, certificate of registered office, certificate of directors and secretary, certificate of registered shareholders, memorandum and articles of association,

ii- Documents of directors and beneficial owners

Identification and personal KYC documents are required from:

- Directors of legal persons.
- Beneficial owners of the legal entity with 10% or more beneficial owners.

These identification documents include proof of identity and proof of residence.

iii- Board Resolution

Resolution of the board of directors of the legal entity for opening the account and granting authority to those who will operate it.

5.3 - Record Keeping Procedures

The Company must retain the information and documents listed below for use in any investigation or analysis of possible money laundering or terrorist financing by national authorities.

Retention of documents/data, other than the original documents or their certified true copies kept in hard copy form, may be in other forms, such as in electronic format, provided that the Company can retrieve the relevant documents/data without undue delay and produce them at any time, upon request, to the competent authorities. A faithful translation is enclosed in case the documents / data are in a language other than English.

a- The name and address of customers and copies or records of official identification documents (such as passports, identity cards or driving licenses).

b- The name and address (or identification code) of the counterparties.

b- The name and address (or identification code) of the counterparties. c- The name and address (or identification code) of the counterparties. d- The account details from which the account was opened.

- d- The details of the account from which the funds were paid.
- e- The form and destination of the payment made by the company to the client.
- f- Business correspondence.
- g- For customer due diligence, a copy of the references of the evidence is required, for a period of at least 5 years after the end of the business relationship with the customer.
- h- For business relationships and transactions, evidence and supporting records for a period of at least five years after the completion of the transactions, or at the end of the business relationship.

5.4 - Notification of suspicious transactions

A suspicious transaction is a transaction that is inconsistent with a customer's known legitimate business or personal activities or with the normal business of the specific account, or in general with the economic profile that the Company has created for the customer.

The Company ensures that it maintains adequate information at all times and knows enough about its customers' activities to recognize in a timely manner that a transaction or series of transactions is/are unusual or suspicious.

5.4.1 - Examples of Suspicious Transactions

Examples of what might constitute suspicious transactions / activities related to money laundering and terrorist financing include, but are not limited to:

- a- Transactions with no discernible purpose or unnecessarily complex.
- b- Use of foreign accounts of companies, or group of companies with complicated ownership structures, which is not justified in terms of the client's needs and economic profile.
- c- Large volume of transactions and/or money deposited or credited to an account, when the nature of the client's business activities does not appear to justify such activity.
- d- There is no visible justification for a client to use the services of a particular financial organization.
- e- There are frequent transactions in the same financial instrument for no apparent reason and under conditions that appear unusual.
- f- There are frequent small purchases of a particular financial instrument by a client who settles in cash, and then the total number of financial instruments is sold in one transaction with cash settlement, or with the proceeds being transferred with the client's instructions to an account other than his own.
- g- There are frequent small purchases of a particular financial instrument by a client who settles in cash, and then the total number of the financial instrument is sold in a transaction with cash settlement or with the proceeds being transferred, with the client's instructions, to an account other than his usual account.

- h- Transactions that do not conform to prevailing market conditions, especially in relation to the size and frequency of the order.
- i- The settlement of any transaction, mainly large, in cash and / or through a third party, who did not give the order.
- j- The settlement of any transaction but mainly large transactions in cash and / or settlement of the transaction by a third party other than the customer who gave the order.
- k- The transfer of funds to and from countries or geographical areas that do not apply or inadequately apply the FAFT Recommendations on money laundering and terrorist financing.
- l- Reluctance to provide complete personal information when establishing a business relationship, i.e., regarding the nature and purpose of their business activities, anticipated account activity, previous relationships with financial organizations, names of their officers and directors or business address.
- m- Provide information that is minimal, difficult or costly for the Company to verify.
- n- Providing unusual or suspicious identification documents that cannot be easily verified.
- o- Frequent or large transactions by a customer with no record of past or present work experience.
- p- Introducing a customer through a foreign financial organization, or a third party whose country(ies) or geographic area(s) of origin do not apply or inadequately apply the FATF Recommendations on money laundering and terrorist financing.
- q- The use of an address that is linked to persons involved in cash transactions, particularly when that same address does not correspond to the declared occupation (e.g. student, unemployed, self-employed, etc.).
- r- Shared address for persons involved in cash transactions, particularly when the address is also a business location and/or does not appear to correspond to the declared occupation (e.g. student, unemployed, self-employed, etc.).
- s- The stated occupation of the customer is not commensurate with the level or size of transactions executed.
- t- Use of general nomination documents in a manner that restricts the control exercised by the company's board of directors.

5.4.2 - Suspicious Transaction Reporting Procedure

The procedure for reporting a suspicious transaction of a customer is as follows:

- a- Reports from Company employees from different departments are evaluated by the AML Compliance Officer.
- b- If deemed necessary, the Compliance Officer will notify the corresponding Money Laundering Authorities.
- c- After the submission of the report, the account(s) of the client in question, as well as any other connected accounts, are closely monitored by the Compliance Officer.

d- After submitting the report, the Company adheres to the instructions given by the relevant Money Laundering Authorities and, in particular, on whether to resume or suspend a particular transaction, or to keep the particular account active.

e- Electronic transactions executed for the client are compared and evaluated against the client's anticipated account billing, regular billing for client activities/operations, and data and information stored for the client's economic profile.

f- Significant deviations are investigated, and findings are recorded in the respective client file.

g- Operations that are not justified by the available information on the client are thoroughly examined to determine if suspicions of money laundering or terrorism financing arise. If this is the case, a report will be sent respectively to the Compliance Officer and then to the relevant Anti-Money Laundering Authorities.

5.5- Daily/Monthly Procedures of the AML Compliance Officer

The procedure that the AML compliance officer must follow on a daily/monthly basis is as follows:

- i. Receive a daily report from staff members regarding any suspicious transactions.
- ii. Review the reports submitted (if any).
- iii. Report to Senior Management and advise on the need to take any of the following actions.
- iv. Halt transactions if reports are in process.
- v. Inform the client of the reasons why their transaction has been canceled.
- vi. Collect transaction information if it has already been executed.
- vii. Report the suspicious transaction to the relevant authorities as per the law.

6. EDUCATION AND STAFF TRAINING

The Company ensures that its employees are fully aware of their legal obligations in accordance with anti-money laundering and counter-terrorism financing laws through a comprehensive employee education and training program.

The training program aims to educate employees on the latest advancements in anti-money laundering and counter-terrorism financing, including practical methods and trends used for this purpose.

The training program ensures that Company employees are fully aware that they may be personally responsible for not reporting information or suspicions regarding money laundering or terrorism financing. The timing and content of the training provided to employees from various departments are adjusted according to the needs of each department.

The frequency of training may vary depending on modifications to legal and/or regulatory requirements, employee obligations, and any other changes in the financial system.



The structure of the training program will be in line with the needs, as well as the various functions, of new employees, existing employees, as well as different departments of the Company.

Ongoing training is provided at regular intervals to ensure that employees are reminded of their duties and responsibilities and kept informed of any updates.

Any personal information collected about the client, such as name, address, date of birth, and contact details, will be strictly maintained by Inverteo for business purposes only. Other information, such as client transactions, copies of passports, and proof of address, will remain confidential and shared only among our account services and compliance departments. Additionally, Inverteo may inquire about the client's creditworthiness, which will also remain confidential within our client files. Such information may be kept physically or electronically with strict access procedures.

Inverteo may share client information with internal departments or affiliated offices performing marketing, back-office, and customer service functions for normal business operations. Each employee within Inverteo has signed a Confidentiality Agreement as client information is required to be kept confidential.

Any questions or additional information regarding our privacy policy can be directed to our Customer Service Department at support@inverteo.com.