

## Anti-Money Laundering and Combating Terrorism Financing Policy

The standards set out in this Policy are minimum requirements based on applicable legal and regulatory requirements and apply for the entire ICM Brokers organization. These requirements are intended to prevent ICM Brokers, its employees and clients from money laundering, terrorist financing or other financial crime. This Policy establishes the general framework for the fight against money laundering and financing of terrorism.

### 1. Introduction

ICM Brokers is committed to the highest standards of anti-money laundering (AML) compliance and requires management and employees to adhere to these standards to prevent use of our products and services for money laundering purposes.

ICM Brokers will examine its Anti-Money Laundering strategies, goals and objectives on an ongoing basis and maintains an effective Anti-Money Laundering program for the institution's business that reflects best practices for a global financial services provider.

Adherence to ICM Brokers Anti-Money Laundering Program is the responsibility of all employees. The program is formulated and directed by the Compliance Officer. The program includes client screening and monitoring requirements, "know your customer" (including the requirement to establish the identity of beneficial owners), Embargo requirements, record keeping requirements, the reporting of suspicious circumstances in accordance with FSA St. Vincent and the Grenadines law, AML employees training besides "know our employee".

If the minimum requirements set out in this Policy cannot be applied in a certain country because application would be against local law or cannot be enforced due to other than legal reasons, ICM Brokers must assure that it will not

- enter a business relationship,
- continue a business relationship or
- carry out any transactions

If business relations already exist in that country, ICM Brokers must ensure that the business relationship is terminated regardless of other contractual or legal obligations.

### 2. Definition

Money Laundering is the introduction of assets derived from illegal and criminal activities (Predicate offenses) into the legal financial and business cycle. Offenses are for example forgery of money, extortionate robbery, drug crime as well as fraud, corruption, organized crime, or terrorism etc. Predicate offenses for money laundering are defined by local law

Money Laundering could happen in several methods and over three principal stages:

#### 2.1 Placement

In the first stage of laundering money, the launderer needs to place the dirty money into the financial system. Large sums are broken down and deposited in one or several banks. Usually, this process will take place in the same country or location where the illegal activity took place.

#### 2.2 Layering

The second step will be to move the funds to give them a legitimate identity and distance them from their source. The launderer will require purchasing investment instruments and securities, executing wire transfers, and opening new bank accounts in different locations in the world. In this stage, the launderer will be seeking stable financial structures without leaving any trace of the source of his funds.

#### 2.3 Integration

In this stage, the funds are already integrated into the financial and monetary system in such a way that they re-enter the financial system as apparently legitimate funds. The launderer will now invest in resources such as real estate, luxury assets, business ventures and large construction / contracting projects, etc...

These “stages” are not static and overlap broadly. Financial institutions may be misused at any point in the money laundering process.

Criminals involved in suspicious activities should never be informed that they are being investigated.

### 3. Minimum Requirements

All ICM Brokers and subsidiaries, if any, must comply with the following basic principles:

#### 3.1 Ascertainment of Customer Identity

- When entering a lasting business relationship
- Obtaining full customer documentation (as detailed in the Account Opening Policy)
- Verifying customer identification, validity, and soundness of the documents
- Verifying the legitimate source of funds deposited by Customers (source of funds should be clearly identified)
- Forbidding the use of anonymous accounts and fictitious names
- Heightened due diligence requirements for politically exposed or other high-risk individuals after obtaining senior management approval to open such accounts
- Checking whether a customer is on the undesirable customers' list (Anti-money Laundering Committee list)
  
- When performing a single transaction or deal,
  - No cash accepting or physical values worth 10.000 USD (or equivalent) outside an existing business relationship, also when performing several smaller payments adding up to this amount (smurfing)
  - Updating customer information
  - Keeping records of transactions for at least ten (10) years following the termination of relationship with the customer.

#### 3.2 Establishment of Purpose of Business Relationship

When entering a lasting business relationship, ICM Brokers must obtain information on kind and purpose thereof, if this is not clear from the business relationship itself.

#### 3.3 Identification of Ultimate Beneficial Owner

Whenever ICM Brokers is required to identify a customer, it must establish and verify the identity of the ultimate natural person,

- Who owns the account or
- Controls the customer or its assets or
- On whose behalf the transaction is carried out or
- On whose behalf the business relationship is established.

#### 3.4 Client Account Monitoring

A suspicious transaction is a transaction that has no business or apparent lawful purpose, is unusual for the customer, or lacks any reasonable explanation. Employees must be aware of the responsibility they hold when conducting their daily tasks. When they know, suspect, or notice any unusual transaction, they should take immediately action and report their suspicion to the designated Compliance Officer.

A permanent monitoring of clients' accounts must be implemented to detect unusual/suspicious transactions. Monitoring must be affected for applicable business areas using adequate processes and systems.

Below are a few indicators that may help employees/ Compliance Officer of ICM Brokers to detect while monitoring suspicious transactions:

- A new or prospective customer is known to you as having a questionable legal reputation or criminal background
- Normal attempts to verify the background of a new or prospective customer prove difficult
- Requests to activate a dormant account
- Deposits of unusually large amounts of money that cannot be justified with the customer's nature of business and/or the customer's history
- Many transactions conducted within a short period of time (i.e. same day) to avoid interrogations
- Receipt of unexpected or unjustified wire transfers (in such cases, investigation should be carried out to know the source of the relevant funds.
- A Customer attempts to purchase investments with cash (cash deposits)
- A Customer wishes to purchase several investments with money orders, traveler's checks, cashier's checks, bank drafts or other bank instruments, especially in amounts that are slightly less than \$10,000, where the transaction is inconsistent with the normal investment practice of the customer or their financial ability
- Transfers of funds or securities between accounts not known to be related to the customer
- Trades conducted by entities that are known sanctioned by regulators in the past for irregular or inappropriate trading activity
- Customer attempts to purchase investments with instruments in the name of a third party
- Payments made by way of third party checks payable to, or endorsed over to the customer
- Transactions made by employees, or that you know are made by a relative of an employee, to benefit unknown parties
- Transactions in which customers make settlements with checks drawn by third parties

### 3.5 Correspondent Banking

Special attention must be paid to correspondent banking business and adequate security measures must be implemented. ICM Brokers will not establish correspondent banking relationships with Shell Banks (banks with no physical presence in any jurisdiction and not affiliated with a regulated body), establish

anonymous accounts or accounts in false names, or maintain an account which is held in the name of one person for the benefit of another person whose identity is not disclosed.

### 3.6 Forbidden Business

Payables through accounts and relationships with shell banks are forbidden for ICM Brokers and ICM Brokers's correspondent banks.

### 3.7 Reporting of Suspicious Circumstances/Transactions

- Determine whether a transaction report requires reporting to an external Anti-Money Laundering Suspicious Cases Unit
- Provide a report to senior management at least annually regarding internal or external suspicious transactions, if any, and ICM Brokers's compliance with applicable laws and regulations
- Address any reported suspicious transaction by undertaking a full and comprehensive investigation, which will ensure the application of all requirements and appropriate reporting
- Prepare adequate training materials (i.e. Q&A) concerning hot cases with regards to AML & CFT
- Update this policy at least once a year as well whenever there is a change in the laws or regulations
- Provide adequate training twice a year on this policy's requirements to all ICM Brokers existing and new staff

Such circumstances/transactions must be reported to the competent authorities according to local law (Anti-money Laundering Committee). No suspicious account will be closed before the Anti-money Laundering Committee is notified of such instances.

### **3.8 Staff Reliability**

ICM Brokers must not employ staffs who are deemed not reliable.

### **3.9 Anti-Money Laundering Controls**

The responsible Anti Money Laundering Officer must ensure that adequate customer and business-related controls with applicable AML requirements are being adhered to and security measures are properly functioning.

### **3.10 Anti-Money Laundering Training**

All employees (including trainees and temporary personnel) responsible for carrying out transactions and/or for initiating and/or establishing business relationships must undergo anti-money laundering training. ICM Brokers has decided to extend the target audience for AML to cover all staff. Initial training must be attended within three months after an employee has joined ICM Brokers, and subsequently on an ongoing basis. Minimum content training requirements have to be adhered to.

### **3.11 Anti-Money Laundering Risk Analysis**

ICM Brokers has set up a system to assess the level of risk exposure considering product and client risk and derive appropriate security measures from this analysis (risk-based approach analysis).

### **3.12 Embargo Requirements**

ICM Brokers will adhere to all applicable embargo requirements and will check clients and transactions against applicable embargo lists.

The Compliance Officer must properly address the situation with confidentiality to the Chief Compliance Officer and simultaneously inform the Board on the course of action.

### **3.13 Checking, Reporting and Freezing Accounts**

In all instances, the Compliance Officer and any individual aware of the ongoing process must NOT inform the concerned parties that they are under investigation and are being scrutinized or possible breach of the AML and CTF requirements. When appropriate, the account must be frozen for proper handling and reporting as required.

## 4. Role and Responsibilities of Staff

### 4.1 Anti Money Laundering Officer

- Responsible for the ICM Brokers's AML & Embargo strategy
- Responsible for escalation and sanction in case of non-compliance of internal and external requirements and lack of quality
- Responsible for the implementation of effective and efficient AML program in line with standards
- Represents AML at Joint Committee and at senior corporate level as appropriate
- Manages AML function, and controls adequacy of organizational structure and resource levels
- Drives communication to the Board with respect to issues concerning AML
- Maintains relationships between AML and the ICM Brokers's external auditors, regulatory and other authoritative bodies
- Oversees AML's budget & ensure that resources for AML are deployed effectively across the region to mitigate high level risk
- Recruits resources in conjunction with Business Management to meet the needs of global and regional plans
- Oversees AML related IT-systems, AML Risk Analysis, change projects, technology, operations, management Information System (Reporting) and all AML-specific processes
- KYC matters, Embargo & Sanction escalations, and any other areas of dispute before further escalation to the legal counsel
- Protects the company from legal, regulatory and reputational risk with regard to business involving sanctioned persons, entities and / or countries
- Conducts staff training
- Responsible for the implementation of adequate monitoring - research /surveillance tools
- Sign-off on the New Product Approvals and Internal Relocation and Outsourcing ("IRO") process as applicable.

### 4.2 Employees

Employees of ICM Brokers must also be on the alert for suspicious transactions that may be indicative of terrorist financing. Anti-Money Laundering programs typically focus on large suspicious cash and non-cash transactions; however, terrorist financing may involve smaller values but can also mimic those of traditional money launderers. Therefore, ICM Brokers employees must also look out for transactions involved in terrorist financing, including:

- Funds generated by businesses owned by nationals of countries associated with terrorist activity
- Charity/relief organization-linked transactions
- Physical currency exchange from countries associated with lax standards of transaction oversight

reporting responsibilities, could lead to criminal charges (significant fines and/or imprisonment).

Employees must refer all requests for information to the designated Compliance Officer immediately. The Compliance Officer will contact the investigating officer and, if deemed appropriate, will authorize disclosure of the information on behalf of ICM Brokers following review with the Chief Compliance Officer, the Board and Legal Counsel.

Persons and entities are protected from criminal and civil legal proceedings for submitting suspicious or prescribed reports in good faith to the competent authority.

## 5. Record Retention

Records must be kept of all transaction data and data obtained for the purpose of identification, as well as of all documents related to money laundering topics (e.g. files on suspicious activity reports, documentation of AML account monitoring, etc.). Those records must be kept for a minimum of 10 years following the termination of relationship with the customer.

## 6. Respecting Privacy and the Confidentiality of Customer Information and Tipping-Off

ICM Brokers respects the privacy and the confidentiality of the information it has on its customers. However, when it comes to combating money laundering and the financing of terrorist activities, ICM Brokers is obliged to disclose certain information to external regulatory authorities. At the same time, ICM Brokers is prohibited from disclosing that it has transmitted such information.

Given the above, employees must be careful not to inform a suspected individual or a third party that competent authorities have been alerted concerning one of his/her transactions, since this disclosure could prejudice a money laundering investigation.

## 7. Updates and Adjustments

This policy and the implemented measures must be reviewed and updated at least on a yearly basis to ensure that all the requirements have been respected. The Compliance Officer is responsible for identifying changes in regulations and assessing the impact on business operations. Additionally, the Compliance Officer, in consultation with senior management, should utilize the assistance of outside counsel, auditors, or other experts the senior management deem necessary to evaluate the compliance and effectiveness of the AML and CTF program.