(INVSTR ADVISORY)
AML / CIP Policy Statement

The anti money laundering (AML), client identification program (CIP) Policy sets standards for identification of customers in order to prevent the use of Invstr products and services for money laundering purposes. The standards set out in this Policy are the minimum requirements based on applicable legal and regulatory requirements. These requirements are created to prevent Invstr, our employees, partners and clients from being misused for money laundering, terrorist financing or any other financial crime, by doing the following:

- Performing enterprise-wide risk assessment to determine the company's risk profile
- Establishing AML policies and procedures
- Implementing internal controls throughout its operations that are designed to mitigate risks of money laundering
- Ensuring know your customer ("KYC") procedures are performed on all users
- Designating a Compliance Officer with full responsibility for the AML Program
- Providing AML training to all employees

1. IDENTIFICATION

At the present time, Invstr is not required to adopt anti-money laundering (AML) policies and procedures. However, the Chief Compliance Officer (CCO) monitors for updates to AML law.

Notwithstanding, Invstr and its partners (We), to whom we introduce Invstr users wishing to carry out investment transactions, adopt a risk-based approach when on-boarding customers in line with current AML/KYC regulations. This document defines how We (in this case, partners) process the registration of customers' accounts, what information is collected and how it is verified.

We identify a customer by obtaining a range of information about them, obtained from reliable sources that are independent of the customer. The following information is received for identification purposes (but not limited to): name and surname; personal identity number (if such exists); date of birth; photograph on an official document which confirms his/her identity; residential address; the number of the personal identification document; the expiry date of the identification document.

Once a customer is identified, and their identity is verified, a certain level of due diligence based on a risk-based approach is carried out. For some business relationships, determined by the firm to present a low degree of risk of money laundering or terrorism financing (ML/TF), simplified due diligence (SDD) may be applied; in the case of higher risk situations,

and specifically in relation to politically exposed persons (PEPs), enhanced due diligence (EDD) measures must be applied on a risk-sensitive basis.

SANCTIONS

Our partners have integrated with electronic data providers to fulfill the regulatory obligations in line with the financial sanctions regime. Information is aggregated from the most important sanction lists (EG. OFAC, EU, UN, BOE, FBI, Bureau of Industry and Security, etc.) worldwide.

POLITICALLY EXPOSED PERSONS

In addition to the aforementioned measures, our partners are integrated with the largest database of PEPs, as well as those of their family members. Whenever a client has been identified as a PEP, enhanced due diligence measures are applied, senior management approval is necessary for establishing, or continuing, a business relationship with such a customer.

2. INTERNAL CONTROLS

NOMINATED OFFICER

Invstr has selected a senior manager to act as Chief Compliance Officer to make the communication between us and governing authorities clearer and more efficient. The key role of the nominated officer is to create a framework where any member of our staff has sufficient skills and knowledge to raise suspicions of money laundering or terrorist financing. Our staff members also have a clear procedure to report their suspicions in due time.

TRANSACTION MONITORING

We use a live transaction monitoring process for the purpose of detecting suspicious activity. As advised by the regulator. We do not rely solely on a set of prescriptive rules and thresholds; instead, We use a risk-based approach, both in alert generation and prioritization. The solution utilizes statistical and analytical techniques to identify patterns of unusual and suspicious behaviors by building profiles on each individual customer and comparing their financial activity against expected and/or peer group norms. This is accomplished by using data analytics tools for flagging anything that falls outside of "normal."

We reserve the right to refuse to process a transaction at any stage, especially when we believe that a transaction is connected in any way to money laundering or any other type of criminal activity. In accordance with the law, we are not obliged to inform the customer that it was reported to the corresponding bodies of the customer’s suspicious activity.

REPORTING

We have established a way in which staff consult with their line managers to provide evaluation for the rationale of further disclosure. By no means does this prevent contacting the nominated officer directly. All internal reports are registered in an appropriate way; the nominated officer maintains a secure suspicious report register. The framework is created in such a way, where a reasonable and faithful evaluation is provided to each report that is received. The nominated officer assesses the risk that is posed by a transaction or activity. In cases where there are associated accounts, an examination of such relationships is to be carried out. If an internal review has indicated enough grounds to know or suspect that any benefit has been acquired and if a criminal property exists, an external suspicious activity report (SAR) is submitted to the relevant national crime agency (NCA).

RECORD KEEPING

Records are kept of all customers' identity, the supporting evidence of verification of identity (in each case including the original and any updated records), our business relationship with them and details of any transactions. As per regulatory requirements, We keep records for at least five years from the date a business relationship ends, or from the date of the last transaction.

TRAINING

We make sure that our employees are aware of the AML program and request that training is provided to all employees (new and existing) before conducting business activities, and, at a minimum, includes:

- Understanding and recognizing money laundering and fraud
- Verifying customer identification
- Identifying suspicious activity and structured transactions
- Reporting requirements related to all transactions

Additional training will be provided regularly to all employees based on, but not limited to, changes in government regulations, Invstr AML Compliance Program requirements, related procedures, and policies, or in the event of a performance issue related to an AML incident.