AML POLICY

วันที่มีผลบังคับใช้ 01.02.2020

1. INTRODUCTION

1.1. The phrase “money laundering” covers all procedures to conceal the origins of criminal proceeds so that they appear to originate from a legitimate source. Investizo LTD. (“Company”) aims to detect, manage and mitigate the risks associated with money laundering and the financing of terrorism. The Company has introduced strict policy aimed on the detection, risk prevention or mitigation in respect of any suspicious activities performed by customers.

1.2. The Company is required to constantly monitor its level of exposure to the risk of money laundering and the financing of terrorism.

1.3. The Company believes that if it knows its client well and understands its instructions thoroughly, it will be better placed to assess risks and spot suspicious activities.

2. CUSTOMER DUE DILIGENCE

2.2. Effective Customer Due Diligence (”CDD”) measures are essential to the management of money laundering and terrorist financing risk. CDD means identifying the customer and verifying their true identity on the basis of documents, data or information both at the moment of starting a business relationship with customer and on an ongoing basis. The customer identification and verification procedures require, first, the collection of data and, second, attempts to verify that data.

2.2. During the Client’s Portal registration process, before obtaining any service from the Company or making any payments to the Company, an individual customers provide the following identification information to the Company:

- Customer's full name;
- Customer's date of birth;
- Country of residence/location of customer;
- Mobile telephone number and e-mail.

2.3. During the Client’s Portal registration process, before obtaining any service from the Company or making any payments to the Company, a corporate customers provide the following identification information to the Company:

- Full company name;
- Registration number and date;
- Country of registration/incorporation;
- Registered address;

- Mobile telephone number and e-mail.

2.4. After receiving the identification information the Company’s staff should verify this information requesting the appropriate documents. The verification process can take up to 4 business days after all requested documents are provided by the Client.

2.5. Appropriate documents for verifying the identity of customer include, but are not limited to, the following:

- For an individual customer: A high resolution scanned copy or photo of pages of a passport or any other national ID, indicating family name and name(s), date and place of birth, passport number, issue and expiry dates, country of issue and Client’s signature;
- For a corporate customer: a high resolution copy of documents showing the existence of the entity, such as Certificate of Incorporation, and, where applicable, Certificate of Change of Name, Certificate of Good Standing, Articles of incorporation, a government issued business license (if applicable), etc.

2.6. To verify proof of address of the customer the Company requires one of the following to be provided, in the same correct name of the customer:

- A high-resolution copy of a utility bill (fixedline phone, water, electricity) issued within the last 3 months;
- A copy of a tax or rates bill from a local authority;
- A copy of a bank statement (for a current account, deposit account or credit card account);
- A copy of a bank reference letter.

2.7. When making a funds deposit or funds withdrawal via credit/debit card a customer is required to provide a scanned copy or photo of the credit/debit card (front and back side). The front side of credit/debit card should show the cardholder's full name, the expiry date and the first six and the last four digits of the card number (the rest of the digits may be covered). The copy or scan of the reverse side of credit/debit card should show the cardholder's signature, but the CVC2/CVV2 code must be masked.

2.8. If an existing customer either refuses to provide the information described above or if a customer has intentionally provided misleading information, the Company, after considering the risks involved, will consider closing any of an existing customer’s account.

2.9. The Regulations measures require further research and identification of customers who may pose a potentially high risk of money laundering/terrorism financing. If the Company has assessed that the business relationship with a customer pose a high risk it will apply the following additional measures:

- Obtaining the information relating to the source of the funds or the wealth of the customer will be required (this will be done via e-mail or phone);
- Seek further information from the customer or from Company’s own research and third party sources in order to clarify or update the customer’s information, obtain any further or additional information, clarify the

nature and purpose of the customer's transactions with Company.

2.10. When obtaining information to verify the customer's statements about source of funds or wealth, the Company's staff will most often ask for and scrutinize details of the person's employment status or business/occupation. The Company's staff will ask for whatever additional data or proof of that employment/occupation that may be deemed necessary in the situation, particularly the appropriate confirming documents (employment agreements, bank statements, letter from employer or business etc.).

2.11. The Company will conduct ongoing customer due diligence and account monitoring for all business relationships with customers. It particularly involves regularly reviewing and refreshing Company's view of what its customers are doing, the level of risk they pose, and whether anything is inconsistent with information or beliefs previously held about the customer. It can also include anything that appears to be a material change in the nature or purpose of the customer's business relationship with Company.

3. PAYMENTS POLICY

3.1. Investizo LTD. requires all deposits, where the name of the originating customer is present, to come from the name matching the name of the customer in our records. Third party payments are not accepted.

As for withdrawals, money may be withdrawn from the same account and by the same way it was received. For withdrawals where the name of the recipient is present, the name must exactly match the name of the customer in our records. If the deposit was made by wire transfer, funds may be withdrawn only by wire transfer to the same bank and to the same account from which it originated. If the deposit was made by means of electronic currency transfer, funds may be withdrawn only by the means of electronic currency transfer through the same system and to the same account from which it originated. To comply with the AML procedures, funds withdrawals have to be made solely in the same currency that was used to make a deposit.

4. PERSONNEL

AML Compliance Officer

4.1. The Company is committed to combating money laundering and for this reason it has appointed a dedicated Anti-Money Laundering Compliance Officer (the "AMLCO") who is accountable to the Board of Directors and Senior Management of the Company.

4.2. AML Compliance Officer's responsibilities include:

- Ensuring the Company's compliance with the requirements of the Regulations;
- Establishing and maintaining internal AML program;
- Establishing an audit function to test its anti-money laundering and combating the financing of terrorism procedures and systems;

- Training employees to recognize suspicious transactions;
- Receiving and investigating internal suspicious activity and transaction reports from staff and making reports to the FIU where appropriate;
- Ensuring that proper AML records are kept;
- Obtaining and updating international findings concerning countries with inadequate AML systems, laws or measures.

Employees

4.3. All Company employees, managers and directors must be aware of this policy.

4.4. Employees, managers and directors who are engaged in AML related duties must be suitably vetted. This includes a criminal check done at the time of employment and monitoring during employment. Any violation of this policy or an AML program must be reported in confidence to the AML Compliance Officer, unless the violation implicates the AML Compliance Officer, in which case the employee must report the violation to the Chief Executive Officer

4.5. Employees who work in areas that are susceptible to money laundering or financing terrorism schemes must be trained in how to comply with this policy or the AML program. This includes knowing how to be alert to money laundering and terrorism financing risks and what to do once the risks are identified.

Employee Training Programme

4.6. The Company provides AML training to employees who will be dealing with customers or will be involved in any AML checking, verification or monitoring processes. The Company may conduct its training internally or hire external third party consultants.

4.7. Each person employed within the Company is assigned a supervisor who teaches him or her in relation to all policies, procedures, customer documentation forms and requirements, forex markets, trading platforms, etc. There is a training plan for each new employee and tests which are being held for 2-3 months (depending on level within the business).

4.8. The Company’s AML training programmes is aimed to ensure its employees to receive appropriate training level with regards to any possible AML/TF risks.

Content of training

4.9. The Company’s AML and risk awareness training includes the following content:

- The Company’s commitment to the prevention, detection and reporting of ML and TF crimes;
- Examples of ML and TF that have been detected in similar organizations, to create an awareness of the potential ML and TF risks which may be faced by the Company’s employees;

- Well known or recognized typologies, especially where made available by the FATF or AML Supervisors;
- The consequences of ML and TF for the Company, including potential legal liability;
- The responsibilities of the Company under the AML Act and Regulations;
- Those particular responsibilities of employees as identified in this AML Policy, and how employees are expected to follow the Company's AML procedures.
- How to identify and report unusual activity that may be a suspicious transaction or attempted transaction.
- The rules that apply against unlawful disclosure of suspicious transactions ("tipping off").

5. ENQUIRIES

For further AML enquiries please contact us at info@investizo.com