ANTI MONEY LAUNDERING POLICY
AND
KNOW-YOUR-CLIENT POLICY
Velarion LLC

1. INTRODUCTION

In response to the international community's growing concern with regard to money laundering and possible financing of terrorism, many countries worldwide enacted or strengthened their laws and regulations regarding this subject. The international regulating bodies have issued a number of recommendations outlining the obligations of companies with regard to money laundering and the fight against terrorism financing. These recommendations encompass provisions applicable to Velarion LLC. (hereinafter- the "Company"). It is the policy of the Company to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements.

The Company commits itself to the highest standards in protecting its business of misuse by Money Laundering (ML) and Funding of Terrorism (FT) or any other criminal activities.

The Company holds license for the operations of online casino games granted by the Antellephone N.V. and is therefore considered a subject person under AML/CFT legislation, namely the National Ordinance on identification when rendering services (LID) and the National Ordinance on the reporting of unusual transactions (LMOT).

The key objective of this policy is to set the structure to prevent that the Companys' services are being misused as a canned for ML, FT or fraudulent activities and that these services comply with the applicable Anti-Money Laundering (AML) and Counter Funding of Terrorism (CFT) rules and regulations which are set in the EU AML Directives, especially Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

This policy is applicable to all employees belonging to the Company and will be reviewed annually and revised as needed.

The Company entities are subject persons to the applicable laws and regulations and will adhere to them in every country where the Company is conducting business in or with.

The Board of Directors and all group employees are required to protect the Company and its reputation by complying with these standards from being misused for ML, FT or other misconduct.

All measures are to be applied on a risk-based approach. The risk-based approach allows the Company, within the framework of the legal requirements, to adopt a more flexible set of measures, in order to target resources more effectively and apply preventive measures, that are commensurate to the nature of risks - to be able to focus our efforts in the most effective way.

By following the risk-based approach, risks in different areas can be identified and measures to mitigate these risks can be applied according to the level of all risks identified. These measures then will be implemented to reflect the day-to-day responsibilities under applicable AML/CFT regulations.

The Company has a zero-tolerance policy for ML, FT or any other financial crime activities.

2. OBJECTIVES

The purpose of this policy is to establish the general framework for the fight against money laundering and terrorism financing throughout the Company and Company's affiliates. The Company is committed to high standards of anti-money laundering / counter terrorism financing (AML/CTF) compliance and requires management and employees to adhere to these standards in preventing the use of its products and services for money laundering or terrorism financing purposes.

This policy established the framework for adequate AML/CFT procedures, AML/CFT trainings and AML/CFT controls, which need to be applied in all business units based on a risk-based approach in order to manage the ML and FT risks of the Company's appropriately.

3. REGULATORY FRAMEWORK

3.1 National regulations

Pursuant to the National Ordinance of Money Laundering (1993), money laundering is a criminal offense. Further main national regulations relating to money laundering and terrorist financing are among others:

The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);

The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G. 2009, no. 65 (N.G. 2010, no. 41) (NORUT) together will all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;

The National Ordinance on Identification of Clients when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2009, no. 66 (N.G. 2010, no. 40) (NOIS) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;

The National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification of Clients when rendering Services. (National Decree containing general measures on Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70);

Sanctions national decree Al-Qaida c.s., the Taliban of Afghanistan c.s. Osama bin Laden c.s., and terrorist to be designated locally (N.G. 2010, no. 93);

National Ordinance on the Obligation to report Cross-border Money Transportation N.G. 2002, no. 74) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations; These laws and decrees serve as the basis for the procedures maintained by the financial sector of Curaçao to detect and deter industry related risks for money laundering, the financing of terrorism or other criminal activities.

3.2 International regulations

On international level, the FATF plays a very important role in the combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction. The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures and promotes the adoption and implementation of appropriate measures globally.

In performing these activities, the FATF collaborates with other international bodies involved in combating money laundering and the financing of terrorism. In total 34 countries are direct members of the FATF and through regional organizations over 180 countries are connected to the FATF.

Subsequently the present policy is a combination of the FATF and local AML/CFT rules and regulations. This ensures a solid, internationally accepted basis regarding AML/CFT. In case local laws and regulations require additional compliance duties, the Company is free to develop additional procedures to comply with local regulations.

4. DEFINITIONS

Money laundering is:

the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;

the concealment or disguise of the true nature, source, location, disposition, movement. rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;

the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;

participation in, association to commit, attempts to commit and aiding, abetting, facilitating And counseling the commission of any of the actions mentioned in the foregoing points.

Terrorism financing is the provision or collection of funds and other assets, by any means, directly or indirectly, with a view to, or in the knowledge that those means will be used in full or in part by a terrorist organization or by a terrorist acting alone, even without any connection to a particular act of terrorism.

5. GOVERNANCE

The Board of Directors has appointed the Money Laundering Reporting Officer (MLRO). To fulfill his tasks, the MLRO has the right to access all necessary data, documentation and information.

The MLRO is reporting directly to the responsible member of the Board of Directors, the Chief Regulatory Officer (CRO) and provides the CRO with regulatory updates on on-going projects and relevant KPIs on a monthly basis.

The AML/CFT program is directed by the MLRO and it is designed to address also related risks in financial crimes and to provide unobscured guidelines for all employees when it comes to prevent financial crimes such as ML and FT.

Within the Company, responsibilities are assigned to designated teams and employees, which support the MLRO in his duties, in order to secure the implementation and the following of Company’s policies and procedures. It is the MLRO’s responsibility to ensure that operational procedures are updated on a regular basis, at least once a year, and will be approved by himself in cooperation with the responsible tram leaders/managers.

To monitor the accordance with legal requirements, the Company established Compliance department developing AML/CTF and KYC procedures, obligatory for all employees of the Company and determining the policy of engagement with clients registered on the Company's website http://www.betitall.bet/ or http://www.pledoo.bet/ (hereinafter - the "Site") and opened an account (hereinafter - the "Clients"; such account: “Client Account”).

6. RISK ASSESSMENT

The Company is required to assess on a yearly basis the risks of money laundering and terrorism financing, taking into account risk factors relating to Clients, countries or geographic areas, products, services, transactions. The Company will collect certain minimum Clients identification information from each Client who opens an account; utilize risk-based measures to verify the identity of each Client who opens an account; record Client identification information and the verification methods and results; and compare Client identification information with government-provided lists of suspected terrorists, once such lists have been issued by the government.

By following the risk-based approach, all possible risk areas and risks can be identified, and mitigating measures are applied according to the grade of risks that have been assessed. These measures will then be implemented to reflect the day-to-day responsibilities under applicable AML regulations.

A business risk assessment and customer risk assessment are performed. The Company implements an going corporate AML/CFT risk assessment to analyze the level of risk that its customers, services, channels, products or geographic locations of its legal entities are posing. The results of the risk assessment lead to appropriate risk mitigating actions.

The Company has set out its comprehensive set of risk mitigating measures in its IT-based AML/CFT Framework of risk assessment, policies, procedures, trainings and controls.

Constant safeguarding of AML/CFT compliance is achieved by designing and installing also controls to manage and reduce the impact of identified risks and to assess the effectiveness and functionality of taken measures.

On an ongoing basis, the MLRO is monitoring the AML/CFT controls to improve their efficiency, proper records of taken actions and the reasoning behind such actions are kept and documented.

Risk Classification
The Company maintains a risk-based approach in relation to its clients in order to effectively detect and deter any risks it may be exposed to such as money laundering, the financing of terrorism or any prohibited transaction such as fraud.

The Company maintains the following risk classification:
- Low risk
- High risk

Low risk
All Clients are classified as Low risk and are subjected to Standard Due Diligence procedures related to the request for KYC documentation as per the process described below and constant monitoring of activities on the account.

High Risk
The Client activity is the determining factor for the classification of a Client as High Risk. Any Client of which an automated alert has been generated or an inappropriate activity has been detected will be categorized as High Risk, for which an Enhanced Due diligence procedure is applied. The instances in which a High risk classification is assigned includes but are not limited to those instances as mentioned in the section below.

The risk associated with the customer can be indicated as a high risk:
- if the customer is non-resident;
- if the customer’s legal structure is complex;
- if the customer is in an industry often exploited for financial crime;
- if the customer’s business is cash-intensive.

Customers can be higher risk if they use nominee shareholders, shares in bearer form, or a company ownership structure that is very complex.

Some customers present higher inherent risk to our organization because of who they are, what they do, the industry they are in, the business they run,or their source of funds or wealth. When assessing the risk posed by a customer, we are checking their status and what they do.

Any customer who will not cooperate, or who refuses to provide satisfactory proof of how the source of funds or source of wealth was obtained, raises a further red flag and become a high risk.

Not all red flags are permanent. We might discover, that our customer has the same name a someone who is listed on an official register for crimes or sanctions. After further investigation, we confirm that our customer is not on that register, we can clear the red flag and hing risk status.

Some jurisdictions are higher risk because their own laws, regulations, and enforcement controls to prevent financial crime are weak, or nonexistent. Higher risk jurisdictions, as defined by the FATF, are countries that have been identified as having strategic deficiencies in their national anti-money laundering and counter-financing of terrorism regimes.

7. KNOW YOUR CLIENT

7.1. Client Identification and Verification:

The Company has adopted a Customer Acceptance Policy in conformity with its obligations as licensed gaming operator to meet all applicable legal requirements such as requirements regarding responsible gaming,player protection and anti-financial crimes. The said policy is not only used for AML/CFT purposes, but also for player protection and is maintained in a separate document.

The Board of Directors and senior management of the Company have established a trong player protection and AML/CFT culture and are constantly communicating a clear message to all employees that the company as a good citizen protects minors and its customers.

The Company adopted a zero-tolerance approach to financial crime or any other ilegal activities to prevents the company from being misused for unlawful purposes. The Company will not tolerate money laundering or funding of terrorism at whatever level, and will not knowingly conduct business with individuals or entities it believes to be engaged in such activities.

Depending on the risk arising from a customer, different levels of customer due diligence (CDD) need to be applied, distinguishing between standard customer due diligence (CDD) and enhanced due diligence (EDD).

Any natural person or corporate entity as business partner shall be identified adequately by full registration of personal/company data, be risk rated and monitored according to the documented processes (procedures) in place.

Personal data such as the official full name, place and date of birth, permanent residential address, identify reference number, where available and nationality should be complemented with information and documentation on the source of wealth/funds as well as any other information obtained by the customer on a risk-based level of CDD. The nature and extent of CDD will depend on the risk presented by the customer, franchise partner or supplier.

The CDD measures also include, besides identifying the customer or business partner, the verification of said customers/business partners based on permissible documentary or electronic sources as well as the identification and documentation of its Ultimate Beneficial Owners (UBOs) and legal representatives where applicable.

No natural person is to be conduct business with, if said does not meet the legal requirements or is prohibited or excluded to use our services for any reasons. No

anonymous or factious named accounts can be opened or obtained. Not more than one active customer account shall be allowed per customer.

Generally, no business can be carried out with any natural person or corporate entity if that subject is suspected to be or confirmedly involved in any relevant illegal activities, especially related to ML, FT or fraudulent behaviors.

In cases of doubt the MLRO must be involved for a risk assessment and initiating appropriate risk mitigating measures if applicable

The Company has established standards regarding Know-Your-Client. These standards require due diligence on each prospective Client before entering into a business relationship:
via identification and verification of his identity and, as the case may be, his representatives on the basis of documents, data or information obtained from a reliable and independent source compliant with the domestic and European anti-money laundering legislation and regulations;
via obtaining information on the purpose and intended nature of the business relationship. Prior to opening an account for the Client the Company will collect the following information for all accounts for any person that is opening a new account and whose name is on the account (hereinafter - the "Preliminary identification"):
the name;
the Client's home country or country of residence or registration;
the Client's IP address.
The Company does not allow its Clients to open anonymous accounts. The Company does not allow its Clients to make any transactions or money withdrawal from the accounts till Complete identification (hereinafter - the "Complete identification").

Prior to allowing any transactions or money withdrawal from the account for the Client the Company will collect the following information about the Client:
the name (name confirmation);
date of birth;
an address, which will be a residential or business street address (for an individual), or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address); and
an identification number or one or more of the following: a taxpayer identification number,passport number and country of issuance, alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard; and
phone number.
The Company has developed a list of documents, the provision of which is necessary for a Client for the purpose of Complete identification, namely:
color passport copy (first and second pages with photo, as well as a page with data of registration);
color copy of a document, which is proper for Client's identity verification under the law of the country of residence;
a copy of driver's license (upon the Company's request);
a receipt of payment of utility bills to confirm the place of residence of the Client (upon the Company's request);
Also the verification process involves mandatory confirmation of Client's phone number.

Based on the risk, and to the extent reasonable and practicable, the Company will ensure that it has a reasonable belief that it knows the true identity of the Client by using risk-based procedures to verify and document the accuracy of the information it gets about Clients. The company will analyze the information it obtains to determine whether the information is sufficient to form a reasonable belief that the Company knows the true identity of the Client (e.g., whether the information is logical or contains inconsistencies).

The Company will verify Client identity through documentary means, non-documentary means or both. The Company will use documents to verify Client identity when appropriate documents are available. In light of the increased instances of identity fraud, the Company will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary.

The Company may also use non-documentary means, if it is still uncertain about whether the Company know the true identity of the Client. In verifying the information, the Company will consider whether the identifying information that it receives, such as the Client's name, street address, zip code, telephone number, date of birth and ID number, allow us to determine that the Company has a reasonable belief that it know the true identity of the Client (e.g., whether the information is logical or contains inconsistencies).

The Company understand that it is not required to take steps to determine whether the document that the Client has provided to the Company for identity verification has been validly issued and that the Company may rely on a government-issued identification as verification of a Client's identity. If, however, the Company notes that the document shows some obvious form of fraud, the Company must consider that factor in determining whether it can form a reasonable belief that the Company knows the Client's true identity.

The Company will use the following non-documentary methods of verifying identity:
Independently verifying the Client's identity through the comparison of information provided by the Client with information obtained from a consumer reporting agency, public database or other source [identify reporting agency, database, etc.];
Checking references with other financial institutions; or
Obtaining a financial statement;
Phone calls to the Client
If a potential or existing Client either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the Company will not open a new account and, after considering the risks involved, consider closing any existing account.

8. INDIVIDUAL RISK ASSESSMENT
The factors taken into account for the individual risk assessment and classification (low or high risk) of Clients on a risk-sensitive basis:
Product, service or transaction risk;
Client risk;
Geographical risk.
Examples of such risk factors that the Company is taking into account to assess Client as an increased risk of ML/TF and for which an enhanced due diligence is applied, are:
the home country or country of residence or registration;
the country of birth;
the nationality;
the profession;
the economic activity;
the appearance on sanction lists;
the PEP-status (politically exposed persons) of Client and representatives;
the delivery channel (face-to-face or remotely with or without safeguards);
the source of wealth;
the type and size of payments that could be expected.
8.1. Clients Acceptance Policy
The Company refuses to establish or to maintain a business relationship if the ML/TF risk related to the business relationship appears too high. Therefore, the Company will not enter into/maintain business relationships if:
It concerns PEPs residing in high risk countries as per Transparency lntemational's Corruption Perception Index (https://www.transparency.org);

It concerns cash, cheques or physical securities without the Client being identified face-to-face or identified remotely with safeguards
It concerns unlicensed/unregulated cryptocurrency platforms, custodial wallet providers or startups launching ICO's;
It concerns arms/munitions dealers;
It concerns unlicensed gambling entities;
It is not satisfied that the MUTF risk can be effectively managed, such as no or insufficient identification and verification of the identity of the Client, his representative(s);
The Client's source of wealth or source of funds cannot be explained (for example through their occupation, inheritance or investments);
The Client, its representative is a person or institution appearing on an embargo or terrorist list issued by EU (https://www.consilium.europa.eu/en/policies/fight-against-terrorism/terrorist-list/), OFAC (https://www.treasury.gov/resource-center/sanctions/) or local authorities;
The Client or anyone associated with him have handled the proceeds from crime;
There is in-house negative information about the Client's integrity, obtained, for example, in the course of a long standing business relationship;
The Client, its representative is a person with whom the Company discontinued the business relationship in the past for AMLTF reasons;
The Client is under 18 years old;
The Client's home country or country of residence or registration is: Australia, Austria, Comoros, France, Germany, Netherlands, Spain, United Kingdom, USA, all FATF Blacklisted countries.
8.2. Ongoing Client Due Diligence
Periodic and risk-based reviews are carried out to ensure that Client-related documents, data or information are kept up-to-date.

8.3. Monitoring of Transactions
Compliance department functions ensure that ongoing transaction monitoring is conducted to detect transactions which are unusual or suspicious compared to the Client's risk profile (expected versus real transactional behavior).

8.4. Record keeping
Records of personal data obtained for the purposes of the prevention of money laundering and terrorist financing are processed and kept in accordance with the EU and local requirements and shall not be further processed in a way that is incompatible with those purposes.

9. MONITORING ACCOUNTS FOR SUSPICIOUS ACTIVITY
The Company enforces its efforts to establish and maintain industry-leading procedures and systems to monitor customer behavior and activities risk-based and on an ongoing basis to sure the detection of any unusual behavior or transactions.

Applicable laws on the prevention of ML and FT require the Company as a licensed gambling company to determine if customers or business partners are Politically Exposed Persons (PEPs) or subject to local or internal sanctions.

PEP and sanctions screening are conducted at the beginning of the customer relationship and going forward on an ongoing basis. PEP/Sanction checks are also carried out manually during EDD investigations, if a customer has been identified as a potential high risk customer.

9.1. Politically Exposed Persons
The requirements relating to PEPs are of a preventive and not criminal nature by law. The Company has an appropriate risk management system in place, including risk-based procedures, to determine:

Whether a customer or the management or the beneficial owner of a business partner is a politically exposed person;
Whether this person can be accepted as a customer and
Which mitigating measures need to be applied.
Generally, a person is politically exposed if he/she holds or has held a prominent public function in the past 12 months. Such prominent public functions shall include, but are not limited to:
Heads of State;
Heads of Government;
Ministers and Deputy and Assistant Ministers and Parliamentary Secretaries;
Members of Parliament;
Members of governing bodies of political parties;
Members of the Courts, or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
Members of courts of auditors, Audit Committees or of the boards of central banks;
Ambassadors charge affaires/diplomats and other high-ranking officers in the armed forces;
Members of the administration, management or boards of site-owned corporations;
Anyone exercising a functions equivalent to those set out in paragraphs above within an institution of the European Union or any other international body.
Close family members, such as:
The spouse or any person considered to be equivalent to a spouse;
Parents and children and their spouses or any person considered to be the equivalent to a spouse are to be classified as PEPs as well
This also applies to persons who are considered “known to be close associates”. This definition applies to every natural person who has joint profits from assets or established business relationship or any other close business relations with a politically exposed person and also natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de fact benefit of a politically exposed person.

A PEP is a politically exposed person. According to FATF there are two types of PEPs:
Foreign PEPs are individuals who are or have been entrusted with prominent public functions be a foreign country;
Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions.
State or heads of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations and important political party officials. Immediate family members. Relatives and close associates may also be classified as PEPs.

9.2. Sanctions
The Company is required to screen customers and on a risk-based level also business partners against sanctions lists issued, among others, be the United Nations, European Union and US Office of Foreign Assets Control (OFAC) at a minimum in all jurisdictions in which the Company operates, unless to do so would conflict with local registration.

Whereas the Company can decide whether to accept PEPs as customers, under no circumstances can business be carried out with any sanctioned natural parson or corporate entity.

9.3. Measures in case of PEP and sanction matches
Company’s relevant operational teams have procedures in place, which describe how to deal with PEP/sanction alerts, identify alerts as false positives or true matches and escalate true matches to the MLRO.

The MLRO have a separate procedure in place, which defines the steps that need to be taken if the designated teams escalate a PEP or sanction match.

According to the escalation procedure,
Senior management approval for the establishment or continuation of a business relationship with a PEP has to be obtained;
EDD measures, including establishment of the source of wealth and ID applicable the source of funds that are involved in such business relationships, need to be applied;
Enhanced, ongoing monitoring of those business relationships needs o be applied.
If a customer is identified as a sanctioned person, the following actions are mandatory:
Immediately freeze all assets held on behalf of the sanctioned person and
Inform the Sanctions Monitoring Board (SMB) to receive further instructions.
The Company will monitor Client's account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to Company's business.

The Red flags are:
the transaction amount is more than 10 000 EUR or equivalent of this amount;
money withdrawal from the account is more than 10 000 EUR or equivalent of this amount;
wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent reason;
transactions patterns show a sudden change inconsistent with normal activities.
If the suspicion arises that multiple Client Accounts have been created in multiple different names or that a Client.
Account is a part of a syndicate of Clients colluding to gain an advantage over the Company, the Company will proceed to suspend all suspicious Client Accounts pending an investigation.

The investigation will consist of the review of playing history, IP location histories including VPN and proxy databases and action to delay ratios commonly displayed with computer sharing technology. If the Company concludes from the investigation that an Account Holder or a group of Account Holders have created multiple accounts and are playing as part of a syndicate of Clients, the Company will proceed to withhold any cash or bonus winnings and reserves the right to withhold deposited funds.

Request for withdrawal:
Withdrawal requests must be made from a Client Account. Withdrawal requests sent by any other means of communication will not be processed. Upon receipt of a request for withdrawal, the Company will request KYC documentation verifying the identity of the Client, in accordance with its internal withdrawal process. The Company will not deposit withdrawn funds to another source from which it was originated. If for any reason this is no longer possible, the Company will request additional verification documentation evidencing the details and ownership of the new withdrawal method. Transfers or pay outs will only be made to the Client. Transfers to third parties are not permitted.

Prior review of account activity:
Before processing any withdrawals, the Company will conduct additional review of the Client Account for any irregular activity such as money laundering or suspicious play such as:
- the placement of a deposit without having placed any bets, or only to receive free spins. A Client must have always placed at least his deposit amount in bets before proceeding to withdraw the funds;
- the possible creation of multiple Client Accounts in multiple different names;
- possible collusion between Clients, detected by the Company’s fraud control system.
Monitoring will be conducted through the automated monitoring system (Compliance Monitoring Program). The Client risk profile will serve as a baseline for assessing

potentially suspicious activity. The Compliance department will be responsible for this monitoring, will review any suspicious activity that Company's monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

10. ORGANIZATION OF INTERNAL CONTROL

10.1 SUSPICIOUS TRANSACTION/ACTIVITY REPORTING (STR/SAR)

Suspicious activities and/or transactions must be identified, handled, escalated and reported promptly.

The Company employees who identify/detect unusual or suspicious activities and/or transactions are obliged to report these incidents to the MLRO immediately. The Company employees can use different ways to submit internal SAR/STRs and are instructed accordingly.

Once an internal report is received, the MLRO and his assignees will indicate the customer's account to assess the unusual behavior and/or suspicion described within the internal report. Based on the outcome of the investigation, the MLRO will decide whether to report the suspicion externally to the relevant authorities or to close the internal report with documented reasons.

Detailed procedures are available for all the departments involved in internal/external reporting on how to investigate internal reports, how to submit reports externally and which risk mitigating measures to take.

The suspected/involved customer or any other third party is not to be alerted of any investigations or reports regarding ML/FT, as under no circumstances a "Tipping-off" is accepted or tolerated, given the fact that this would be a serious criminal offense.

The MLRO is obliged to reports any suspicious activity or transactions to the respective authorities where the MLRO knows, suspects or has reason able grounds to suspect ML/FT promptly. The internal or external reporting of a suspicious activity cannot be suppressed.

The Money Laundering Reporting Officer (MLRO) is in charge of the reporting with the relevant authority and will hold a list of all instances in which it did not consider it necessary to report. The decision not to report will be sufficiently supported. In case the report is filed with the FIU or any internal investigation is taking place, the Client shall not receive any of this information.

10.2. Procedures

All the Company's departments have implemented AML/CTF rules into operational procedures, taking into account their type of activities, their volume and their size together with the local legal and regulatory requirements.

10.3. Training

The Company developed a coherent training program, including follow-up trainings on a regular basis (in-class trainings, E-learning, webinars), in order to create and maintain a satisfying AML/CTF awareness.

Adequately AML/CFT trained staff is a cornerstone of every effective AML/CFT program to protect the company of related risks. It created also the level of awareness that is key to report any suspicious activity without undue delay.

New employees shall receive anti-money laundering training as part of the mandatory new joiners training program (as applicable in their respective company).

All employees are required to complete a web-based AML/CFT training annually. Employees its operational or other substantial AML responsibilities shall receive additional AML/CFT trainings as applicable, especially if they are responsible for the maintenance of customer relationships or for processing transactions.

10.4. Compliance Monitoring Program

In order to assure the effectiveness of instructions, procedures and processes, recurrent quality controls are performed in the AML/CTF-domain pursuant to the Compliance Monitoring Program.

10.5. Staff Due Diligence

It is imperative that the Company's employees are of undisputed integrity. To ensure this objective, the Company follows a procedure whereby all applicants must produce a curriculum vitae, at least two references and relevant educational qualification certificates, and/or professional certificates, which are checked and verified by the Company's Human Resources Department.

The Company ensures the review of employees for their reliability with qualified measures, through employee control and appraisal systems during the hiring process and on an ongoing basis during the time of employments by management evaluation.

10.6. Record Keeping

All identification documentation and service records shall be kept for a minimum period of no less than five years after the termination of the contractual relationship with the customer notwithstanding retention periods of other laws as e.g. tax or data protection laws.

AML/CFT relevant data in relation to internal investigations, KYC measures or STR/SARs shall be obtained for five years and, if no further bid is identifies, deleted after.

All data and documentation shall be made available to authorized persons promptly on request and without undue delays. Authorized persons are e.g. competent authorities or public prosecutors, the FIAU/FIU, etc.