General

1.1 Policy statement

It is the policy of UAB Aureus Labs that all staff members actively participate in preventing UAB Aureus Labs services from being exploited by criminals and terrorists for money laundering purposes or used to finance terrorist activity through profits obtained through the use of the company's website. This participation has the following objectives:

Ensure compliance by UAB Aureus Labs with all applicable laws, statutory regulatory instruments and the requirements of the relevant supervisory body.

Protect the company and all its employees as individuals from the risks associated with infractions of the law, regulations and supervisory requirements.

Preserve the good name of UAB Aureus Labs against the risk of reputational damage that involves involvement in money laundering and terrorist financing activities.

Contribute positively to the fight against crime and terrorism. To achieve these goals, the UAB Aureus Labs policy is that:

Each employee must fulfill his personal obligations as appropriate to his role and position in the company.

Business considerations will never take precedence over UAB Aureus Labs's commitments to combat money laundering.

The company will appoint an Money Laundering Reporting Officer (MLRO) and a designated staff member to continue during his absence, and will have the full assistance and cooperation of all staff members in the performance of their duties. appointments. Any reference to the MLRO in this document will include the designated staff member in case the MLRO is temporarily absent.

1.2 Definition

UAB Aureus Labs believes that, before applying its Fraud Management Procedure, it is essential to identify what, on the one hand, money laundering is, and what constitutes, on the other, terrorist financing.

Money laundering consists of moving or hiding the proceeds of crime to cover up the connection between crime and the funds generated, in order to benefit from the proceeds of crime. Thus, the ultimate goal is to cover up the origin of the funds.

Terrorist financing is the process of providing funds or other assets, directly or indirectly, to terrorist groups or individual terrorists to support them in their operations. This can occur through funds from legitimate sources or from a combination of legal and illegal sources. In fact, funding from legal sources is a key difference between terrorist organizations and traditional criminal organizations involved in money laundering operations. While it seems logical that there is no need to launder funding from legitimate sources, terrorists often have a need to cover up or disguise the links between the organization, or the individual terrorist, and its legitimate sources of funding.

2. The risk-based approach

2.1 Definition

In accordance with applicable law, UAB Aureus Labs takes a risk-based approach. Thus, it identifies and analyzes its risks and subsequently makes use of measures, policies, controls and procedures to curb any unwanted risk, among which those related to the risks of money laundering and terrorist financing materialize. This approach allows UAB Aureus Labs to exercise significant flexibility and discretion. This in itself implies significant responsibility. It is up to UAB Aureus Labs to demonstrate through appropriate documentation, which includes but is not limited to a risk analysis process, that it has evaluated all risks and properly applied all measures to control them. In this sense,This policy establishes the specific measures that UAB Aureus Labs will adopt to guarantee that its conduct complies with the Risk-Based Approach regarding the consideration and identification of risks that directly affect money laundering and terrorist financing. .

2.2 Risk assessment

Risk Management implies

i) recognition of the existence of a risk

(ii) conduct a risk assessment, and

(iii) apply systems and strategies to manage and control the identified risks.

There is no doubt that the distance business is considered risky. However, the risk assessment will identify the main risks facing the company, as well as the level of those risks, so that, consequently, the necessary measures can be taken to manage and control the identified risks. This procedure will specify the controls and processes that must be followed to ensure that the risks that UAB Aureus Labs has identified and that it will face in the framework of its operations do not materialize. The organizational risk assessment of UAB Aureus Labs, which must be approved by the Board of Directors, takes into account the following factors:

i. Product / service / transaction risk

Some products / services / and transactions are more vulnerable to criminal exploitation than others. These include any product or services offered

ii. Interface risk

It refers to the channel through which UAB Aureus Labs establishes a commercial relationship and / or through which transactions are carried out. Non-face-to-face interactions, as in the case of the commercial interface of UAB Aureus Labs, are no longer automatically considered high risk, provided that technological measures and controls are adopted to deal with the high risk of impersonation or identity fraud. UAB Aureus Labs will adopt a good combination of document-based verification methods and electronic sources, as mentioned below, to counter the above risks. For example, although UAB Aureus Labs makes use of electronic databases, it is aware that the databases only confirm that the identification data provided corresponds to that of a real person, and not that the user is really that person. Providing additional identification documents will provide additional evidence that UAB Aureus Labs had reason to believe that the user is indeed the person he claims to be.

iii. Geographical risk

This is the risk to UAB Aureus Labs of the geographical location of customers, but also the geographical location of their providers and service providers. The element to consider in relation to this fraud management procedure is mainly attributable to customers and the origin of their funds. The user’s nationality, residence and place of birth must be taken into account, as they may be indicative of a high geographic risk. Also in the terrorism faction - countries that are known to suffer a significant level of corruption, countries subject to international sanctions related to terrorism or the proliferation of weapons of mass destruction, will be considered high risk. The opposite is also true and thereforethey can be considered medium or low risk.

Risk assessments are "work in progress". These evaluations must be constantly reevaluated as new risks arise. Risks can arise due to changes in technology, which can facilitate money laundering or terrorist financing attempts. Other changes include expanding the customer base or adding services and payment methods that present a different risk profile than those already offered, which will require a review of the business risk analysis. In such changes, UAB Aureus Labs will reevaluate business risks at least once a year to discuss whether any changes are necessary. When determining the level of risk of a user, the accumulation of all indicators will be taken into account. Altogether, these determine the user’s risk profile.

iv. Customer risk

Refers to the type of customer the service is provided to. The evaluation of the risk presented by an individual is generally based on the economic activity and / or the source of wealth of the individual. By identifying the level of risk inherent in a relationship, UAB Aureus Labs will assess the likelihood that a customer could launder the proceeds of crime through the UAB Aureus Labs service. A high-income customer who spends a quarter of his monthly salary on gambling is unlikely to be a high risk, even if the amount wagered is large. In contrast, a user with a minimum wage who spends his only salary on gambling or any high risk material can indeed constitute a high risk. In addition, the person will be examined to determine if he is a politically exposed person (PEP),or if it is associated in any way with a PEP. It will also be verified that the person is not subject to sanctions or other legal measures.

3. Customer due diligence (CDD)

3.1 Procedure

The Fraud Management Procedure will now focus on the procedure of knowing the customer and identifying the risks related to their transactions and the origin of their funds, both where the funds were obtained and their source.

As described above, a risk assessment can never be a one-size-fits-all exercise. In this sense, UAB Aureus Labs will carry out a risk assessment when entering into a business relationship. The aforementioned risk assessment will allow UAB Aureus Labs to develop a risk profile in relation to the user and classify the risk as low, medium or high, which will allow them to identify the controls to be adopted. The user's risk profile will not be filled out at the time of registration. The registration part of the process will only mean the start of the information collection, so the risk profile will be expanded and improved as the relationship with the user develops. In terms of the change in identified risk, the measures taken to control the risk will have to be adapted accordingly. In addition, ongoing monitoring, as explained in more detail below, will ensure that any changes in risk are detected as soon as possible. The level of supervision will be proportional to the risk presented by the specific user , but systems will be available to detect developing risk situations. It will ensure that any changes in risk are detected as soon as possible. The level of supervision will be proportional to the risk presented by the specific user, but systems will be available to detect developing risk situations.It will ensure that any changes in risk are detected as soon as possible. The level of supervision will be proportional to the risk presented by the specific user, but systems will be available to detect developing risk situations.

For starters, UAB Aureus Labs takes CDD steps to determine who its customers are. All the details collected in the registration phase are used to build the user's profile and also on the particular aspects of behavior. This aspect of the profile will help determine the risk associated with the particular user and, therefore, will also facilitate the identification of future unusual behaviors. The CDD is divided into the following three parts:

3.1.1 Customer identification and verification

Identification consists of collecting the user's personal data. This information is collected during the registration process. The personal information collected is to start the Know Your Client (KYC) procedure, which includes the collection of the following personal data:

A. Name and surname

B. Permanent residence address

C. Date of birth, since the user must be over eighteen years of age (or any other age applicable in the specific jurisdiction of the user).

D. Valid email address

E. Place of birth

F. Nationality, and

G. Identity reference number, if applicable.

Once the above information has been provided, UAB Aureus Labs will first check whether the person in question is a Politically Exposed Person (PEP), a PEP family member or a close PEP business partner. To do this, a trusted electronic database will be integrated and used, such as opensanctions.org and Veriff. If an individual is determined to be a PEP or related in any way to a PEP, the individual will be considered a PEP in himself and will not be able to register as a user in UAB Aureus Labs, since UAB Aureus Labs has a policy strict not to accept PEPs as users. This means, therefore, that determining whether a person is a PEP (as defined above) will take place in the registration phase.

The account will be formally opened as soon as the user's email is verified. In any situation where the user is immediately identified as high risk, UAB Aureus Labs may immediately request additional personal data and verification thereof. In any case, UAB Aureus Labs will ensure that it can determine at all times who the customer claims to be and that the measures taken are sufficiently effective to neutralize the risk of identity theft and impersonation.

Verification consists of confirming the personal data collected for identification purposes through the use of independent data, information and documentation obtained from reliable sources. If inconsistencies are detected in the personal information provided by the user, UAB Aureus Labs will study additional identification and verification measures.

This will happen in two ways:

i. Documentary sources

As a general rule, this method of verification will be carried out by referring to government-issued documents containing a photographic image along with the user's identity (for example, passport, identity document, driving license). If the user’s address cannot be verified by any of the aforementioned documents, UAB Aureus Labs will request reliable alternative documents, such as a recent utility bill, bank account statements, government or public entity correspondence, etc. in order to carry out the verification. The requested documents will be received by email and, if deemed necessary, notarial documents may be requested.

UAB Aureus Labs will ensure that all documents received are clear, readable, of good quality and authentic or reflect authenticity. Some documents, such as passports, may be easier to verify because they can be compared to others. In other cases, such as utility bills, the verification process may be less easy. UAB Aureus Labs will perform additional checks using specific software applications or programs that will be integrated as a solution to help get the job done.

In relation to the validity of the information provided, UAB Aureus Labs will also take into account other data collected from the user, such as the geographical location, the data of the IP address, etc., which in normal circumstances should corroborate the data contained in the documents provided by the user. There will be exceptions, when the IP address does not match the country / location. These cases must be verified on a case-by-case basis and verification / clarification will be obtained directly from the user

ii. Electronic media

They include sources such as E-ID or Bank-ID and commercial electronic databases. UAB Aureus Labs is aware that the reliability of these databases is not always optimal. In this regard, it will take into account which source of information is being entered into the database and whether this data is known to be generally updated. When using the aforementioned electronic databases, UAB Aureus Labs will also use other documentary evidence for better confirmation / reliability. This is because a positive result in the electronic database will only mean that there is a person whose personal data coincides with those provided by the user, but not that the user is that person. On the other hand, when using electronic sources such as E-ID and ID-Bank,which can only be accessed through the use of the credentials of a specific person, no additional means of verification will be requested because these sources are considered a sufficiently strong link.

3.1.2 Obtaining information on the purpose and expected nature of the business relationship

The purpose of opening an account is quite obvious and therefore no clarification will be sought on the reason for the request to open an account. However, there may be a hidden reason for opening the account, possibly for money laundering or terrorist financing. If UAB Aureus Labs has any suspicion that such a hidden motive exists, it will conduct an additional investigation and request additional data and documentation to justify its suspicions or confirm that, in fact, there are no justifiable indications of an illegal motive.

There is no specific period or period in which these additional checks will be performed, as they will simply be carried out when suspicion arises. Therefore, they may need to be done in the registry, while in other cases they will have to be carried out until the specific mandatory anti-money laundering thresholds are reached.

In the event that checks are made before the mandatory period, UAB Aureus Labs will first collect sufficient information and, if necessary, documentation to establish the user's source of wealth. The source of wealth is to determine the activities that generate the user's net worth, which will lead UAB Aureus Labs to determine if this amount of wealth justifies their projected and actual level of account activity, and if the user is within the risk matrix (according to the table in the next section). When the risk determined after the checks is medium or low, UAB Aureus Labs will accept a customer statement with details such as the nature of the job / business and a statement on the annual salary. Surveys will also be used on professional networks and social media for verification purposes. If the risk is high or UAB Aureus Labs has doubts about the veracity of the information collected, the user will be asked to provide more independent and reliable documentation that demonstrates the alleged source of wealth. Thus, for example, the individual may be asked to submit a copy of his payroll or to provide any other documented evidence confirming his statement. The individual may be asked to submit a copy of their payroll or to provide any other documented evidence confirming their statement. The individual may be asked to submit a copy of their payroll or to provide any other documented evidence confirming their statement.

B. Continuous monitoring

Ultimately, it is about monitoring customer transactions, their personal data and changes in their circumstances or betting preferences, to ensure that they are consistent with the planned activity and, if not, identify why they have occurred. the changes. The goal is to subjectively identify and analyze large unusual transactions, changes in patterns, and other "unusual" activities. In this regard, it is important that UAB Aureus Labs ensure that information about user's is kept up to date. This will encourage and even compel user, through the terms and conditions, to inform UAB Aureus Labs of any changes and possibly to provide documentation confirming it. Through the monitoring process,the level of risk will be analyzed and it will be determined whether the previously established risk classification should be modified or not. Any inconsistency in the information must be justified and UAB Aureus Labs reserves the right to request more evidence to corroborate it.

Adequate continuous monitoring also involves carefully examining the user's transactions and patterns to ensure that they match the user's knowledge of UAB Aureus Labs, the users activity, and his risk profile. If both do not match, UAB Aureus Labs will question the situation in the same way. Whenever UAB Aureus Labs requests more information, it will take note of its conclusions to demonstrate its compliance. In the event that any inconsistencies detected persist without having been satisfactorily resolved, UAB Aureus Labs will study the advisability of presenting a report to the competent authorities and will also make a decision on whether it considers it necessary to suspend the user's account.

Finally, when it comes to PEPs, it may be the case that a user has not been considered a PEP in the registration phase, but becomes a PEP during the business relationship. If UAB Aureus Labs is aware of such a change, UAB Aureus Labs will end their business relationship as it has a strict policy of not accepting PEP as user's. If, for one reason or another, the person has not been identified as PEP, even if it was in the registration phase, but is identified as such, UAB Aureus Labs will cancel any profit made by the person. You will then transfer the deposited funds to the original source from which the funds come. Consequently, it will close the user's account, according to the procedure described in section 3.3 below.

3.2 Time and application of CDD measures

As described above, the user's account will be opened successfully once the user has registered providing the requested basic personal information. The system is configured to avoid the registration of minors, rejecting any date of birth entered that means that the user is under eighteen years of age (or any other age according to specific legislation - as in Latvia - 21 years).

Verification of any user's data (with the exception of PEP confirmations) may be done at any time at the discretion of UAB Aureus Labs. However, as a minimum, it must be carried out when the amount deposited by the user's reaches the accumulated amount of 1,000 euros. It is indifferent that these deposits have been made through a single transaction or several apparently linked transactions or not. Therefore, UAB Aureus Labs will implement a system that will calculate daily if the user' has reached the deposit limit of 1,000 euros in his account. Another important factor that the system will include is the identification of possible multiple accounts, whose accounts would have been created specifically to defraud the company through abuse of bonuses or specifically to never reach the required deposit limit of 1,000 euros and thus ensure that the account remains under verification.
Until this limit is reached, UAB Aureus Labs will carry out continuous monitoring in accordance with section 3.1 B above to ensure that user information remains correct. Furthermore, if UAB Aureus Labs notifies inconsistencies between the information provided by the user and any other information acquired at any time, UAB Aureus Labs will question the discrepancies and take the corrective measures it deems necessary. In addition, in case of suspected money laundering or terrorist financing, it will follow the procedure established in section 4 below.

Once this threshold is reached, the user's risk profile will be confirmed based on the risk assessment carried out under point 2.2. In addition, if thirty days have elapsed since the threshold of 1,000 euros was reached and the user has not provided the requested information and / or documentation, UAB Aureus Labs may end the business relationship with the user by following the procedure established in the next section.

Risk identified Measures taken

Low

- Verification of personal data

- Continuous monitoring is performed to ensure that the relationship remains low risk and the limit is not exceeded again

- Any suspicion of money laundering or terrorist financing should be reported

- Additional personal data that UAB Aureus Labs considers necessary are collected

- Verification of personal data is done through documents containing photographs of the individual

Medium

- Information on the source of wealth and funds is collected

- Continuous monitoring is performed to detect unusual activities, as well as to keep information and profile updated

- Any suspicion of money laundering or terrorist financing should be reported

- Additional personal data that UAB Aureus Labs considers necessary are collected

- Verification of personal data is done through documents containing photographs of the individual

High

Information on sources of wealth is collected

Continuous monitoring is performed to detect unusual activities, and also to keep information and profile up to date. Fund sources may need to be determined for specific transactions UAB Aureus Labs will allow users to continue using their account while still obtaining the necessary information and / or documentation from the user in question. However, until UAB Aureus Labs

does not effectively obtain the aforementioned information and / or documentation, and verifies the user's identification, it will not allow the user to make any withdrawal of funds from his account, regardless of the amount in question. The user has not provided the requested information and / or documentation UAB Aureus Labs will end the business relationship with the user by following the procedure described in the next section.

3.3 Termination of the business relationship

UAB Aureus Labs will end your business relationship with a user if the user does not provide the information and / or documentation that UAB Aureus Labs has repeatedly requested. UAB Aureus Labswill void any winnings and transfer the deposited funds to the original source from which the funds were