

KYC Policy

Cyber Labs B.V.

Customer Risk Assessment (CRA)

After the identity verification of a client, a risk profile is formed based on the clients'

behavioural patterns. This behavioural pattern is examined through the transaction activity and the type of game-play the client opts for. The CRA is also carried out throughout the business relationship.

After the behavioural pattern is analysed, every customer is given an internal classification as defined by the Customer Risk Assessment (CRA). If suspicious behaviour is observed, evidence will be recorded on the customer profile, and Enhanced Due Diligence (EDD) is applied.

Customers undergo an ongoing ML/FT Risk Assessment from the start of the business relationship and thereafter based on:

- customer type;
- products/services used (e.g. sportsbook);
- transactions/payment systems;
- delivery channels; and
- geographical origin of the customer and/or payment method.

Upon registration, a customer's activity will undergo ongoing monitoring through automatic and manual processes to establish a risk profile, which is essential to enable the casino to apply a certain level of Customer Due Diligence (CDD), commensurate to the ML/FT risk posed. This monitoring is maintained, and the risk level may be reconsidered, depending on changes in customer's activity and to establish the point of reaching the relevant due diligence requirements thresholds. A customer's risk profile is key in obtaining relevant information pertaining to the customer, and maintaining a constant diligence on customer risk.

On the basis of the CRA the appropriate level of CDD can be applied, as stipulated in the Client Acceptance Policy (CAP).

10. Client Screening

An overview of the Client screening is provided in this policy; kindly also refer to the PEP, Sanctions and Negative Media Policy for more information.

As a licensed entity, the company recognizes the importance of the customer profile and has in place practices to comply with the laws and regulations concerning identification, verification and screening of the Client for sanctions, political exposure and negative media . Upon initiation of the first deposit within the account registration, the Client will be immediately screened using a third party provider K36/CMD and block any Clients who are

a positive PEP, Sanction or negative media match. Following registration, the company's list of Clients is automatically scanned by K36/CMD on a weekly basis .

Positive matches and those Clients who cannot be discounted as a positive match on the information provided by K36/CMD shall be investigated through open sources to obtain further information about the match and immediately inform the MLRO by following internal reporting procedures. The MLRO may appoint anyone within the department to investigate such matters. The company reserves the right to request further documentation concerning any possible match in order to verify or discount the suspicion. If a positive match is confirmed due to the match meeting several criteria, such matches will be reported to the relevant authority. The following criteria are applicable for a match to be determined as a positive:

- Name and surname
- Date of birth
- Nationality

The MLRO has the responsibility of ensuring that the screening is being carried out as instructed; to achieve this, sampling of the data shall be carried out and recorded accordingly.

9.1 PEP / Sanctions Lists Checks

Customers are also to be screened to confirm that they are not included on Sanctions Lists. Customers are asked on first deposit to confirm whether the customer is him/herself, or is a family member of, or known associate to, a person that is considered a Politically Exposed Person ("PEP") being both domestic or international PEP. The customer is further checked to confirm PEP status once the relevant thresholds are hit, or the customer's profile is considered to be higher than low risk. PEP screening is carried out prior to the initial engagement.

Customers matching any one of these categories are to be automatically considered as a high-risk profile and appropriate measures taken to ensure that the business activity with them is not of an ML/FT nature. Sanctioned individuals cannot be accepted as customers. Refer to **PEP / Sanctions Lists Procedure** and **Customer Acceptance Policy**. PEP and Sanctions List checks will be carried out against the software K36/CMD.

It is the reporting entity's responsibility to perform ongoing checks of its client database against the international lists of designated persons/ entities/ groups to make sure the reporting entity is not permitting/ facilitating access to funds to the ones mentioned on the sanctions lists. The primary sanctions list reporting entities must check against are UN, EU, USA-OFAC lists (expanded below), local lists of all jurisdictions where online gaming and gambling activities are provided and/or clients are accepted, and/or any other lists applicable at present, and/or which may become applicable from time to time.

Instances of sanctions screening:

- during initial client/player registration;
- daily;

The Company shall ensure that it shall not do business with terrorists or suspected terrorists, or other sanctioned persons or companies. Published lists should be checked, being as follows;

- US Treasury Office of Foreign Assets Controls Specially Designated Nationals and Blocked Persons Lists
- EU sanctions lists
- For PEP's: Transparency International Corruption Perceptions Index/
www.knowyourcountry.com

Although due diligence is required for every PEP, as measures required may vary, and the level of diligence is different according to scenarios, such as:

- Type of function carried out by the PEP
- The country from which the PEP originates
- The transactions that the PEP carries out

In the case of PEP's, the termination of the PEP although stipulated at 12 months after resignation, will be assess for further political involvement or possibility of being a close associate with.

9.2 Negative Media

Negative media shall be deemed as information or intelligence, whether proven factual or alleged, related to serious financial crime, Terrorism, fraud, narcotics, or any crime that has an element of or could lead to ML/FT. Negative Media Screening is to be conducted when establishing a business relationship with a Client. Instances where a Client is connected to Negative Media, will be evaluated prior to granting a business relationship.

When analysing Negative Media hits, we are looking at individuals that are both convicted and not fully convicted, meaning; allegations, cases under investigation pending the legal procedure, wanted individuals and any intelligence which gives rise to knowledge or suspicion that the Client is involved with ML/TF.

Negative Media hits showing predicate offences of ML such as mafia, forgery, drug trafficking and fraud and terrorism amongst many others, shall be reported due to the sensitivity of the crime and the involvement of financial crime. Should any predicate offence raise concerns, they shall be raised with the MLRO or Deputy accordingly.

Negative Media is categorised as follows:

i) Financial Crime

- Financial crime covers a wide range of activities, including ML and the FT. It may also include fraud, bribery, or insider trading. Financial crime is a broad and complex criminal field that may be covered in both traditional and emerging media.

ii) Violence

- Violence involving Clients directly, or carried out on their behalf, may generate significant different types of adverse media, especially when part of a criminal enterprise. Violent crimes may be associated with political and workforce disputes, or wider patterns of human rights abuse.

iii) Terrorism

- The financing of terrorism, any terror-related activities are liable to generate significant adverse media across a range of media outlets. Terror-related types of adverse media may range from the distribution of terrorist literature and encouragement to radicalization, to the direct perpetration of terrorist acts.

iv) Fraud

- Fraud can be perpetrated in numerous ways and includes fraudulent letters, telephone calls, emails, and websites. Fraud can be both a civil and criminal offence and, while the majority of cases involve improper financial gain, it may also involve property or immigration.

v) Narcotics

- Narcotics crimes involve not only the use or sale of drugs but also drug production and trafficking. Narcotics offences and associated news stories are often related to financial crimes, including ML and FT.

vi) Cybercrime

- Any criminal activity involving a computer or networked device like a phone or tablet may be considered cybercrime and reported as such. Cybercrime is an umbrella-term describing activities used to facilitate other offences like digital financial crime, ML, fraud, and terrorism.

vii) Regulatory

- Regulatory misconduct or non-compliance may constitute a crime in itself, or be an indication that Clients are involved in other types of criminal activity. The types of adverse media stories relating to regulatory offences frequently cross-over with financial crime.

viii) Property

- Adverse media stories on property may involve activities such as burglary, theft, larceny, and arson, and constitute both civil or criminal misconduct. Property offences may vary greatly in scope and be reported in a wide variety of news media formats.

ix) Trafficking

- Trafficking involves the transport of humans for the purposes of forced labour or sexual exploitation. A serious criminal offence, trafficking is often related to other offences, including terrorism and various financial crimes.

x) Sexual Crimes

- Sexual crimes include a wide range of activity, from violence, abuse, and rape to the transmission or possession of illegal imagery. Sexual crimes are often in proximity to other offences, including ML and cybercrime.

Any of the offences indicated above, whether convicted or alleged, shall be evaluated and terminated accordingly if the media is deemed to be a positive match.

11. Risk Factors specific to the Gambling Sector

There are 4 risks which the BRA and CRA cover as a minimum. These are:

Customer risk

This is the risk of ML/FT which arises from maintaining relations with a given person. The assessment is generally based on the individual's economic activity and/or Source of Wealth (SOW). categories of customers who may pose a higher risk are as follows:

- Customers having multiple sources of income
- Customers with irregular income streams
- PEP's
- High spenders (as money can be derived from illegal activities)
- Disproportionate spenders (spending is inconsistent with the Company's knowledge of the individual's SOW)
- Improper use of third parties, use of others to avoid CDD measures and scrutiny
- Unknown customers
- Junkets

To this end, the Company sets an upper value of the customer's probable spending power, which if reached, will trigger further checks.

Geographical risk

This is the risk posed to the Company by the geographical location of the player and the SOW of the business relationship. Nationality and place of residence must be taken into account as the player may hail from a jurisdiction having lax AML laws, and also being a haven for terrorists. The Company consults the following sources for further information on the risk the player may pose;

- Countries on FATF list of high-risk jurisdictions subject to a Call for Action
- Countries on FATF list of jurisdictions under increased monitoring
- Countries on CFATF public statement
- Countries identified as jurisdictions of concern or primary concern in the US Department of State annual international narcotics control strategy report (INCSR).
- Countries on the European Commission list of third countries having strategic deficiencies in their AML/CFT regime
- Countries sanctioned by OFAC
- Countries identified by credible sources as hosting terrorist organisations within them
- Countries on the corruption perception index (Transparency International)
- The MLRO compiles a list of countries considered as high risk or low risk.

Product, Service and Transaction Risk

Some products are riskier than others, and pose a higher chance of ML/FT occurring through their use, through the use by customers and the acceptance of casinos of specific payment methods. These include:

- Proceeds of crime - money from narcotics, theft etc
- Anonymous payment methods (such as use of Virtual Financial assets etc)
- Use of casino accounts - these are only allowed to be used for gambling purposes and not to withdraw or deposit with minimal play
- Types of specific games (ex: roulette, craps).
- Peer to peer gaming
- Use of customer accounts held in third party names
- Transfer of funds from one account to another
- Identity fraud
- Electronic wallets - not all e-wallets are licensed, and some jurisdictions accept deposits to e-wallets in cash.

The Company employs its best diligence in order to avoid situations such as the above from occurring within its corporation. The Company, together with the MLRO compiles a list of products which are considered as posing more of a high-risk, and employs measures in order to mitigate that risk, accordingly.

12. Risk Assessment - A dynamic approach

The Company conducts a risk assessment to assess ML/FT risks whenever a new product is introduced. This is done whenever:

- A new product is developed
- A new business practice emerges