



ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

Before the provision of any services to a client, identification of a prospective client must be made from documents issued by reliable sources as prescribed in the NOIS and whenever applicable/possible the directors, representatives or Ultimate Beneficial Owners of the prospective client must be interviewed personally. The operators are also required to obtain and document information on the purpose and intended nature of the business relationship with their (prospective) clients prior to offering them any services.

To prevent and combat money laundering or the financing of terrorism, the operator shall conduct standard customer due diligence which shall, at least, include the following:

- the identification of the client and the verification of the client's identity;
- the identification of the ultimate beneficiary and taking reasonable measures to verify the identity of the ultimate beneficiary in such a way that the service provider is convinced of the identity of the ultimate beneficiary;
- measures to establish the objective and the envisaged nature of the business relationship;
- conducting ongoing checks of the business relationship and the transactions carried out during this relationship, in order to ensure these, correspond to the knowledge the operator has of the client, his/her/its business and the ultimate beneficiary, as well as their risk profiles, including, if necessary, the origin of the financial resources; and, e. measures to establish whether a client is acting for him/her/itself or on behalf of a third party and taking measures to establish and verify the identity of the third party.

Furthermore, operators are encouraged to perform antecedent screening on persons subject to CDD. This could be done by e.g. searching the internationally accepted authoritative lists on the internet.

10.1. Individuals

The employees, the Agents and persons acting on behalf of the Company shall strictly comply with the CDD requirements for opening and operating of any account. No anonymous accounts or accounts in fictitious names shall be permitted, and all individuals opening an account must be over the age of 18. The Network Service Partner understands that allowing persons below the age of 18 to bet on its platform is an offense under various Relevant Laws.

The Compliance Officer shall perform CDD when:

- a) A player wagering stake, or collecting winnings (including the withdrawal of funds deposited) exceeds GBP 2,000 or more (whether the transaction is executed in a single operation or in several operations which appear to be linked); and/or
- b) A player's activity has been identified as suspicious by the Company, MLRO, the Network Service Partner or their officers and employees responsible for ensuring compliance with the AML Policy and the CDD Procedure.

If a person refuses to cooperate for a period of 28 days, even when they have been explained the reasoning behind the regulatory ask the Network Service Partner should terminate the business relationship and report the same to the MLRO or the Compliance Officer (as applicable) as withholding information is one of the "red flags" that could indicate that criminal activity has taken place and that the laundering of the proceeds of these crimes could be attempted.



ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

Client's categories

- *High Risk clients*

High risk clients include:

- I. politically exposed persons;
- II. clients from countries which inadequately apply Financial Action Task Force's recommendations;
- III. correspondent banking relationships with clients from third countries;
- IV. any other client determined by the Company itself to be classified as such (please refer to appendix 1).

- *Normal risk clients*

All clients that do not fall in the low or high-risk categories are considered as normal risk clients.

Face-to-face CDD

When conducting face-to-face CDD or executing transactions for which instructions have been received on a face-to-face basis, the operator must:

1. provide a copy of the original identification document or the original transaction document with the text: "Mr. and or Mrs. appeared to me in person"; and a stamp with the prevailing date; and
2. add the signature of the client as well as the name and signature of the employee who performed the CDD or executed the transaction, to the original document.

Age Verification and Identification of (prospective) clients

The Network Service Partner does not allow customers under the age of 18 or older if local laws so stipulate as applicable to gamble and has systems and monitoring in place to ensure as far as practicable that underage customers aren't able to create accounts and gamble.

Network Service Partner shall abide by the license issuer rules and regulations pertaining to underage gambling and to any specific product rules issued by suppliers of gambling products.

If on completion of verification the customer is shown to be underage:

Their account will be frozen

The status of the account will be set to "Closed" and a note placed on the account

All wages will be treated as void and any deposits made will be refunded to the form of payment used. Where this is not possible, a parent or guardian must give details of an alternative payment method.

The verification and identification process includes:

That the customer is not able to continue with the registration until the "over 18" or "over 21" as applicable checkbox is checked.

The date of birth registration field doesn't allow for an input below the age of 18 or 21 as applicable with a pre-calculated algorithm.

Confirming the customer's identity by checking public available records where available; or



ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

Confirming the customer's identity by having them provide a valid government-issued photo ID such as a passport or driving license when there is a suspicion that the customer is maybe underage through customer interaction and game play activity behavior, or
Warning potential customers that underage gambling is an offense
Requiring customers to affirm that they are of legal age
Periodically reviewing its age verification systems and implementing local industry standard improvements that may be made as technology advanced and as information improves
Ensuring that relevant staff are properly trained in the use of any age verification procedures; in particular customers services staff must be trained appropriately
Carrying out secondary age verification checks in any circumstances which give the operator reason to suspect that the person may be underage

Document verification: based on the knowledge and understanding obtained during the interactions with potential customer, the Network Service Partner shall establish the following:

B2C: In case of individuals, the Network Service Partner shall require the following:

- Full name of the customer
- Government issued identification documents containing a photograph including Passport, Social Security Card, Tax registration cards, driving license etc.
- Existing mailing and residential address along with the proof thereof.
- Contact numbers
- Nationality
- Date of Birth

B2B: For verification of the identity of the legal entity, the Network Service Partner shall require the following:

- Full business name of entity
- Business Incorporation or registration number
- Existing registered and mailing business address
- Contact details of the authorized representatives
- Date and place of incorporation and certificates evidencing the same
- Charter documents and the AML policies and procedures adopted by the company if any
- Full name, ID, Address, Date of Birth, Nationality of all Directors/Partners having executive authority of the entity.

Pursuant to article 3 of the NOIS, the identity of clients must be established through one of the following valid documents:

- a driver's license;
- an identity card issued;
- a travel document or passport;
- other document to be designated by the Minister of Finance.

Ongoing CDD

The efforts to "know your customer" must continue once the client has been identified, even after the initial identification of the client. While the on-going due diligence process must also include



ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the operator's knowledge of the client, its business and risk profile, and where necessary, the source of funds. In the event that doubts relating to the identity of the client arise after the client has been accepted, the relationship with the client must be re-examined to determine whether it must be terminated and whether the incident must be reported to the FIU.

The operator should apply CDD requirements to existing customers and may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction.

Examples of when it may otherwise be an appropriate time to do so is when:

- (a) appropriate scrutiny of transactions and other activities to ensure that they are consistent with the operator's knowledge of the customer, the customer's business and risk profile and source of funds for the transaction;
- (b) there is a material change in the way that the account is operated;
- (c) customer documentation standards change substantially; and
- (d) the operator becomes aware that it lacks sufficient information about an existing customer.
- (e) monitoring whether the customer or any known beneficial owner is listed on the sanctions list.
- (f) operator identifies any unusual activity, which should:
 - perform appropriate scrutiny of the activity;
 - conduct enhanced customer due diligence; and
 - consider whether to make an internal disclosure.

In the latter instances, updated copies of the identification document must be collected and retained.

Furthermore, the operator should ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of clients or business relationships.

Identification of Politically Exposed Persons

The law defines "politically exposed persons" as:

"the natural persons that have or had been entrusted with prominent public functions in the republic of Curacao or any other country, as well as their immediate family members or persons known to be close associates of such persons"

The operator has appropriate risk management in place to determine whether it's (proposed) clients are considered political exposed persons ("PEP's) and conduct enhanced due diligence for politically exposed persons (PEPs), their families and associates. The operator's decision to enter into business relationships with a PEP must be taken at its senior management level. The operator makes reasonable efforts to ascertain that the PEPs source of wealth and source of funds/ income is not from illegal activities and where appropriate, review the customer's credit and character and the type of transactions the customer would typically conduct. The operator must not accept or maintain a business relationship the institution knows or must assume that the funds are derived from corruption or misuse of public assets. Where a customer has been



ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, institutions must obtain senior management's approval to continue the business relationship. Where the operator is in a business relationship with a PEP, it must conduct enhanced ongoing monitoring on that relationship.

In addition, enhanced checks are applied if the country of origin of the PEP is widely known to be corrupt and where AML legislation may not be fully adhered to by the jurisdiction in question. Therefore, the operator categorizes the jurisdictions of clients and list the jurisdictions, which are considered most vulnerable to corruption e.g., those who do not apply the 40 requirements of FATF. As regards corruption, the operator uses Transparency International Corruption Perceptions index, Moneyval, IMF, FATF and World Bank as appropriate sources of information.

The meaning 'Politically Exposed Persons' includes the following natural persons who are or have been entrusted with prominent public functions' in any other foreign country:

- I. heads of State, heads of government, ministers and deputy or assistant ministers
- II. members of parliaments
- III. members of the governing bodies of political parties
- IV. members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances
- V. members of courts of auditors or of the boards of central banks
- VI. ambassadors, chargés d'affaires and high-ranking officers in the armed forces
- VII. members of the administrative, management or supervisory bodies of State-owned enterprises.
- VIII. Directors, deputy directors and members of the board or equivalent function of an international organization
- IX. Mayors

Without prejudice to the application, on a risk-sensitive basis, of enhanced Client due diligence measures, where a person has ceased to be entrusted with a prominent public function within the meaning above for a period of at least one year, the Company shall not be obliged to consider such a person as politically exposed.

None of the categories set out in above shall be understood as covering middle ranking or more junior officials. 'Immediate family members' includes the following:

- (a) the spouse or the person with which cohabit for at least one year
- (b) the children and their spouses or the persons with which cohabit for at least one year
- (c) the parents.

'Persons known to be close associates' includes the following:

- (a) any natural person who is known to have joint Beneficial Ownership of legal entities or legal arrangements, or any other close business relations, with a person referred to in above
- (b) any natural person who has sole Beneficial Ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the person referred to in above.

Without prejudice to the provisions of the Manual, the operators adopt the following additional due diligence measures when it establishes a Business Relationship or carry out an Occasional Transaction with a PEP:

- (a) the MLRO shall use a screening software to run the player's entries against sanction lists, legal regulatory directions, law enforcement lists, negative news, adverse media, local and



ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

international government records etc in respect of sanctioned persons/entities. The MLRO may use any procedures necessary to determine whether a prospective Client is a PEP. These procedures may include, depending on the degree of risk, the obtaining of information from the Client himself or from publicly available information.

- (b) the decision for establishing a Business Relationship or the execution of an Occasional Transaction with a PEP is taken by an Executive Director of the operator and the decision is then forwarded to the MLCO. When establishing a Business Relationship with a Client and subsequently it is ascertained that the persons involved are or have become PEPs, then an approval is given for continuing the operation of the Business Relationship by an Executive Director of the Company which is then forwarded to the MLCO
- (c) before establishing a Business Relationship or executing an Occasional Transaction with a PEP, the operator shall obtain adequate documentation to ascertain not only the identity of the said person but also to assess his business reputation (e.g. reference letters from third parties)
- (d) the operator shall create the economic profile of the Client by obtaining the information specified above. The details of the expected business and nature of activities of the Client forms the basis for the future monitoring of the account. The profile shall be regularly reviewed and updated with new data and information. The operator shall be particularly cautious and most vigilant where its Clients are involved in businesses which appear to be most vulnerable to corruption such as trading in oil, arms, cigarettes and alcoholic drinks.

The data and information that are used for the construction of the Client-legal person's economic profile shall include, inter alia, the following:

- the name of the individual
- the country of origin
- the permanent residential address
- financial information – Source of Funds and Source of Wealth
- existing banking relationships of the individual;
- international or home country telephone directory;
- the products that offered to the client
- Searching the internationally accepted authoritative lists on the internet.
- Transactional History

- (e) the account shall be subject to annual review in order to determine whether to allow its continuance of operation. A short report shall be prepared summarizing the results of the review by the person who is in charge of monitoring the account. The report shall be submitted for consideration and approval to the Board and filed in the Client's personal file.

If an individual is Suspected to be on the PEP list, we will request:

1. Player's KYC and
2. Player's ID with real time face (if needed)

Once we have the provided documents and confirm player is a PEP, we will identify the account as a PEP, ensure the account is classified as High Risk, complete the uptake of Enhanced Due Diligence (EDD) from the player and Report to MLRO if any suspicions. If not a PEP, no action is taken, but will continue to monitor.



ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

Sanctions Policy

Assigned Compliance Officers will conduct screening on a weekly basis on all new players and checks through all player databases and the owners and directors of business participants. Individual's registered name, date of birth, address and locations will inspect to identify any match information from PEP & Sanction Lists.

The operator shall take reasonable measures to comply with sanctions and restrictive measures ("Sanctions") imposed on countries, territories, entities or specific persons and bodies by the United Nations, the European Union, United Kingdom as well as by the US Department of Treasury Office of Foreign Assets Control ("OFAC").

- The operator will adhere to the directives and guidance from the regulatory and other competent authorities relevant to sanctions that have a jurisdiction over operator.
- The operator will abstain from business relationships or transactions which violate or facilitate a violation of Sanctions as defined in this Sanctions Policy.
- With respect to persons and entities subject to Sanctions in general the Gaming Operator:
 - Will not establish a new business relationship
 - Will not facilitate significant transactions
 - In case of existing clients, will follow the instructions and guidelines provided by the Regulated Authority with direct jurisdiction over the operator that may require:
 - To suspend/terminate business relationship with the client;
 - To report the client/business relationship to appropriate authorities;
 - The Company could consider entering into and maintaining a business relationship with a client related to or affiliated with a sanctioned person, however such client will be subject to enhanced due diligence, frequent open source, database checks and transaction monitoring.
- The company should focus enhanced counterparty diligence and screening exercises on areas of the company's business that carry a greater likelihood of involvement with sanctions targets, or their agents, for example:
 - Where there is reasonable cause to suspect that any counterparty derives its profits from activities prohibited under international sanctions measures.

If an individual is Suspected to be on the Sanction list, we will request:

- Player's KYC and
- Player's ID with real time face (if needed)

Once the player's KYC are received, the MLRO will informed to confirm whether the player is a match with the Sanction list or not. If yes, the account will immediately be suspended, and the authorities will be informed. If not on the Sanction List, no action to be taken. The account will be monitored.

10.2. Enhanced CDD for high-risk categories of customers

Enhanced due diligence (EDD) shall be performed for all Politically Exposed Persons (PEPs), their immediate family members, and close associates. PEPs will be identified through initial onboarding and periodic screening. Relationships with PEPs must be reviewed annually, with approvals required at the senior management level. Additional documentation on source of wealth and funds must be collected and verified.