

ComeOn Curaçao N.V.

**ANTI-MONEY LAUNDERING & PREVENTION
OF TERRORIST FINANCING POLICY**

Document Control Table

Classification	Owner	Approved by
Highly confidential	MLRO	Executive Management

Document History

Author	Approver	Date	Revision History	Version
MLRO	Executive Management	07/08/2021	Creation	1.0
MLRO	Executive Management	20/07/2022	Policy review	1.1
MLRO	Executive Management	23/06/2023	Policy review	1.2
MLRO	Executive Management	08/03/2024	Policy review	1.3

Table of Contents

Table of Contents	3
1. Acronyms and Definitions	5
2. Objective and Purpose	6
3. Overview	7
3.1 What is Money Laundering and Terrorist Financing?	7
3.1.1 Placement	7
3.1.2 Layering	8
3.1.3 Integration	8
3.2 What is Funding of Terrorism?	8
4. Business Risk Assessment	9
4.1 Customer Risk	9
4.2 Geographical Risk	10
4.3 Product Risk	11
4.4 Transaction Risk	11
4.5 Interface Risk	12
5. Customer Risk Assessment	12
5.1 Customer risk factors and levels	13
5.1.1 Low Rsk	14
5.1.2 Medium Risk	15
5.1.3 High Risk	15
6. Customer Due Diligence (CDD)	16
6.1 What is CDD?	16
6.2 When is CDD Performed?	16
6.3 How is CCD Performed?	16
6.3.1 Identification	16
6.3.2 Verification	17
6.3.3 Inability to Carry Out CDD	18
7. Enhanced Due Diligence (EDD)	18
7.1 What is EDD?	18
7.2 When is EDD Performed?	18
7.3 How is EDD Performed?	19
7.4 Source of Wealth (SOW)	20
7.4.1 What is the Source of Wealth?	20
7.4.2 When is a Source of Wealth check performed?	20
7.4.3 How does the Company review SOW documentation?	20
7.5 Source of Funds (SOF)	21
7.5.1 What is the Source of Funds?	21
7.5.2 When is a Source of Funds Check Performed?	21

7.5.3 How does the Company review the Source of Funds?	21
7.5.4 Inability to obtain EDD	22
7.5.5 Acceptable Documentation Guide	23
8. Politically Exposed Persons (PEPs)	25
8.1 PEPs Individuation and Mitigation	25
9. Sanctioned Individuals	26
10. High Risk and Sanctioned Jurisdictions	26
10.1 Directive (EU) 2015/849):	26
10.2 FATF: High- Risk countries subject to a call for Action October 2022:	27
10.3 Jurisdictions considered by FATF with strategic deficiencies as updated in October 2022:	27
10.4 UN and EU sanctions:	28
10.5 OFAC sanctions:	28
11. Ongoing Monitoring	28
12. Match Fixing	30
13. Training	31
14. Review	32

1. Acronyms and Definitions

AML	Anti-Money Laundering
CDD	Customer Due Diligence
Company	ComeOn Curaçao
CTF	Countering Terrorist-Financing
EDD	Enhanced Due Diligence
KYC	Know Your Customer
MLRO	Money-Laundering Reporting Officer
PEP	Politically Exposed Person
RBA	Risk-Based Approach
SAR	Suspicious Activity Report
SDD	Simplified Due Diligence
SOF	Source of Funds
SOW	Source of Wealth
STR	Suspicious Transaction Report

2. Objective and Purpose

The purpose of this Anti-Money Laundering & Prevention of Terrorist Financing Policy (the 'Policy') is to set out the obligations of the Company in light of the AML and CFT regulatory framework, and the measures, policies, controls, and procedures to be adopted by the Company to ensure compliance with such regulatory framework.

The Company is committed to the highest standards of AML compliance, and requires its management and employees to adhere to these standards. The senior management of the Company is fully engaged in the processes around the assessment of risks for money-laundering and terrorist-financing, and is involved at every level of the decision making to develop the Company's policies and processes for the Company to comply with the relevant laws.

The standards set out in this Policy are minimum requirements based on applicable legal and regulatory requirements. These requirements are intended to prevent the Company, its employees, and its customers from being misused for money laundering, terrorist financing, or other financial crime.

The Company examines its anti-money laundering strategies, goals and objectives on an ongoing basis and maintains an effective AML programme for all its business, reflecting best practices for an online gaming Company. The programme covers customer screening and monitoring requirements, KYC policies, record-keeping requirements, reporting of suspicious circumstances in accordance with relevant laws and AML training.

The risk-based policies and procedures that were created, cover the following main points:

- Customer due diligence (CDD) measures and ongoing monitoring, including enhanced measures for high risk customers;
- Reporting;
- Record keeping;
- Internal control;
- Risk assessment and management;
- Training; and
- The monitoring and management of compliance with, and the internal communication of, such policies and procedures.

The Company, as a provider of remote games of chance, must ensure that its gambling operations comply with all the applicable laws, regulations and guidance, including the Prevention of Money-Laundering Act and its subsidiary regulations. The Company must also ensure that effective monitoring of compliance and enforcement can be carried out by the competent authorities.

3. Overview

3.1 What is Money Laundering and Terrorist Financing?

Money laundering is the process by which the illegal nature of criminal proceeds is concealed or disguised in order to lend a legitimate appearance to such proceeds. Traditionally, three stages were identified for the purposes of money laundering: the placement stage, the layering stage, and the integration stage.

3.1.1 Placement

In the placement stage money derived from illegal activities is often initially introduced into the financial system by breaking up large amounts of cash into less conspicuous smaller sums and placing these funds into circulation through formal financial institutions and other legitimate businesses, both domestic and international. This is the point at which the proceeds of crime are most apparent and most easily detected. This is the most vulnerable stage in the laundering process.

3.1.2 Layering

Once the money has been placed in the financial system, the launderer engages in a series of conversions or movements of the funds to distance them from the source. This second stage involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to obfuscate the source and ownership of the funds.

3.1.3 Integration

In the third stage, the launderer seeks to bestow apparent legitimacy to illicit wealth through the re-entry of the funds into the economy in what appears to be normal business or personal transactions. The funds would be invested in legitimate businesses or other forms of investment (e.g. investing such funds into real estate, luxury goods, or business ventures) therefore enabling the funds to enter the economy in a legitimate manner.

This three-stage model is rather simplistic and does not accurately reflect every type of money laundering operation. In fact, a modern explanation of money laundering moves away from the traditional three-stage concept and focuses more on the concealment or disguise of the origin of the illicit money.

Remote-gaming companies are subject persons. This points at the legislator's awareness of the probability that remote gaming may be used in order to launder funds. Online gambling may be a target for criminals and this could manifest itself in the following non-exhaustive behaviours:

- Players deposit a (large) amount of money in a player's account and then request a pay out
- Players deliberately lose a (large) amount of money to another player without having played to any significant extent
- Money acquired through crime is laundered through participation in games of chance, with a certain loss being accepted. If the money is laundered, it can be spent freely and the risk of detection by public authorities is reduced. The loss is regarded as a cost incurred in order to dispose of the laundered money
- Criminals spend money gained through criminal activities as a 'reward' for their criminal activities (consumer money laundering)

3.2 What is Funding of Terrorism?

Funding of terrorism is the process by which terrorist organisations or individual terrorists are funded in order to be able to carry out acts of terrorism.

The funding of terrorist activity, terrorist organisations, or individual terrorists may take place through funds deriving from legitimate sources or from a combination of lawful and unlawful sources. Indeed, funding from legal sources is a key difference between terrorist organisations and traditional criminal organisations involved in money laundering operations. While the former may thrive on funds derived from legitimate sources, money laundering necessarily involves funds derived from illegal sources. Another difference is that while the money launderer generates income by obscuring the link between the crime and the generated funds, the terrorist's aim is not to generate income from the fund-raising mechanisms but to obtain resources to support terrorist operations.

Although it would seem logical that funding from legitimate sources would not need to be laundered, there is nevertheless often a need for terrorists to obscure or disguise links between the organisation or the individual terrorist and its or his legitimate funding sources. Therefore, terrorists must similarly find ways to process these funds in order to be able to use them without drawing the attention of authorities.

Some of the specific methods detected with respect to various terrorist organisations include cash smuggling, structured deposits to or withdrawals from bank accounts, purchases of various types of monetary instruments, use of credit or debit cards and wire transfers.

4. Business Risk Assessment

4.1 Customer Risk

The customer risk posed to the Company is determined when taking into account the below five heads of risk. These are dealt with individually in this document, however, a short summary is being included next to each risk for completeness of this section:

1. Registration and verification: the Company only accepts customers who would have completed its registration process, either through its deposit-and-play method or else through the traditional registration form method. The details provided on registration are then verified either on registration itself by means of BankID or else when the customer reaches the statutory €2,000 in deposits on his gambling account. EDD measures are undertaken whenever it is established that certain behaviour / transaction / activity on the account requires more in-depth investigation as to the reason behind it and the origin of the means by which it was conducted.

2. PEPs: when the Company detects an account holder to be a real PEP either through the check on registration or through the check as part of the ongoing monitoring, the account is immediately closed. The Company does not have a risk appetite for PEPs to hold a gambling account therewith.
3. Financial sanctions: Similar approach to the PEP procedure. The Company is also aware that if there had to be a positive genuine hit when checked against a sanctions database, the Company is bound to inform the Sanction Monitoring Board immediately.
4. Corporate customers: The Company does not accept legal persons as customers. Only natural persons are allowed to hold a gambling account and they must always do so in their own name.
5. Third-party service providers: The Company seeks to contract with reputable providers in order to assist it with carrying out certain checks including, for example, PEP checks (provided by LexisNexis).

In a nutshell, the Company's customer acceptance policy dictates that the Company does not provide its services to the following:

- Customers who do not provide identification details;
- Customers who already have a registered account on a given brand;
- Customers who fail to provide the Company with documentation when requested to do so;
- Customers who are on any sanction lists referred to as part of the procedures of the Company; and
- Clients who are identified as PEPs.

4.2 Geographical Risk

The geographical risk is the risk posed to the Company by the geographical location of where it offers its gambling services. It is acknowledged that countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction as well as countries which are known to have terrorist organisations operating within are to be considered as high risk. The geographic risk is two-fold:

1. Jurisdiction: Aware of the geographical risk that certain countries may pose, the Company only takes players from reputable jurisdictions. To this effect, the Company does not allow registrations from countries on the EC or FATF list of high-risk or blacklist or greylist jurisdictions.

2. IP address: The customer's location is traced by means of IP-address detection. On registration, any mismatch between the country selected as a residential country and the IP address blocks the registration altogether.

4.3 Product Risk

This is the risk that the Company is exposed to by means of the nature of the product offered and the risk could be divided in two:

1. Product type: the Company offers both sportsbetting, casino slots games, and live casino. Sportsbetting is considered to be a medium risk, in fact, a section on match-fixing is included in this policy in order to address such a risk. All the slots games offered are RNG-certified and provided by reputable providers. Although live casino is normally considered higher in risk, the player still plays against the house and with the exception of roulette, the risk posed is significantly lower than peer-to-peer games (e.g. poker). The Company does not offer any poker games to the customers.
2. Bonus schemes: The Company invests in promotional campaigns in the form of bonuses. The Company is aware that there is a high risk of abuse of such scheme; notwithstanding it employs a score-based system in order to detect bonus abusers.

4.4 Transaction Risk

The Company makes use of a number of payment providers and payment methods in order to enable its customers to deposit on and withdraw from their gambling accounts. Transaction risks arises from the following categories of risk:

1. Multiple accounts: only one account per player per brand is allowed. The registration process deploys the following criteria to detect duplicate accounts:
 - a. same name + surname + post-code
 - b. same name + surname + home address
 - c. same email address
 - d. same phone number
2. Payment methods: the Company seeks to offer secure and reliable payment methods. It is understood that certain payment methods pose higher risks than others. The Company's risk in this area lies in the provision of prepaid cards and the possibility of crypto deposits.¹ Withdrawals after prepaid-cards deposits and

¹ The Company does not accept crypto currencies but only receives FIAT currencies after they would have been independently converted into FIAT from crypto; and only remits FIAT currencies which would then be converted into crypto.

crypto deposits are assessed more rigorously to mitigate the inherent risk associated with these methods.

3. Payment providers: the Company seeks to contract with reliable payment providers who are duly licensed.
4. Chargebacks: The Company seeks to minimise the risk of chargebacks by requesting copies of cards, limiting active cards on the gambling account to three and asking for fresh KYC from the customers.
5. Ongoing monitoring of customers: the Company acknowledges that the risk of the customer may change in the duration of the business relationship. Transactions are constantly monitored by our fraud tools in order to instantly detect and alert us about irregular transactions. Amongst others, deposit amounts, volumes, changes in depositing patterns, specific BINs and specific IBANs are all taken into consideration as part of the constant screening of customer transactions.

4.5 Interface Risk

This risk may be defined as the risk arising out of the interface used to establish and maintain a business relationship and/or to carry out transactions and the delivery channels used. Interacting with customers on a non-face-to-face basis need not be considered as automatically presenting a high risk of ML/TF, if systems are implemented to address the risks of impersonation or identity fraud, which would otherwise make the interface risk consideration as high.

5. Customer Risk Assessment

Risk weighting and risk assessment are an integral part of the current AML/CFT regime. Each customer represents different levels of risks in terms of ML/FT. The level of AML/CFT measures which the Company is obliged to apply to each customer must be commensurate with the level of risk posed. The higher the risk weighting, the higher the level of AML/CFT measures. Consequently, the basis of the current AML/CFT regime is the identification and assessment of risks and the implementation of policies and procedures to address them. Therefore, the approach that must be undertaken by the Company in relation to the AML/CFT rules is a flexible application to the circumstances in line with the risk assessment.

The establishment of risk is important in order to take appropriate measures to mitigate such risks. The legislation itself acknowledges that resources are finite and it is to this

extent that the Company channels its resources where higher risk lies. This is by adopting a risk-based approach.

5.1 Customer risk factors and levels

Each customer is risk assessed and the outcome of the risk assessment may be a risk rating of high, medium, or low. Each risk rating will have a number of parameters which will cover the four risk pillars (customer, geographic, interface and product).

Risk Level	Type of Customer	Transaction Risk	Product Risk	Geographical Risk
Low	Registered and verified players via bank ID; Fully verified players; Non-PEP; Non- sanctioned players; Registers through a verified affiliate site; Long-standing customer	Low deposits of under €50 per week; Using reputable EEA based payment service providers; Using verified cards; Using bank transfers of which a bank statement is on file	Casino slots	EU/EEA member state or a member of FATF without any monitoring
Medium	Customers tagged as bonus abusers	Customer registered for more than 3 months spending €2,000 in 24 hours	Sportsbook, live casino with the exception of roulette	Non Reputable Jurisdictions
High	PEPs; Sanctioned persons; Individuals who do not provide identification details;	Customer registered for under 3 months, deposits in rolling 24-hour periods €2,000 or more;	Certain gameplay on roulette	Call to Action FATF List, Increased Monitoring Risk List

	Customers who do not provide requested documentation.	Any customer who deposited over €20,000 in 1 week; Any customer who deposits over €30,000 lifetime; Customer using crypto currency as a deposit method; Customer using prepaid cards; Attempting withdrawals without waging the deposit		
--	---	---	--	--

Table 1: Customer-risk factors

This table illustrates the risk factors taken into consideration for the customer risk assessment. The risk is considered cumulatively, but the end risk profile will be set on the basis of the factor triggering the highest risk level.

5.1.1 Low Risk

- i. Registered and verified players via bank ID;
- ii. Fully verified players;
- iii. No hits on PEPs/sanctions check
- iv. Registration is tracked to have come through a verified affiliate site;
- v. Long-standing customer
- vi. The customer deposit a maximum of €50 a week;
- vii. The customer register a low risk funding method;

- viii. Customers register on the system through affiliate links; and/or
- ix. Customers are mainly betting on Casino slots games
- x. Customers are registered to have an address from reputable jurisdictions.

5.1.2 *Medium Risk*

- i. Customer has been registered for more than 3 months spending €2,000 in 24 hours.
- ii. Any customer who deposited over €20,000 in 1 week;
- iii. Any customer who deposits over €30,000 lifetime;
- iv. Sportsbook stakes; and/or Table Games such as Blackjack and baccarat
- v. Customer coming from non-reputable jurisdiction

5.1.3 *High Risk*

- i. Customer registered for under 3 months, deposits in rolling 24-hour periods €2,000 or more;
- ii. Any customer who deposited over €20,000 in 1 week;
- iii. Any customer who deposits over €30,000 lifetime;
- iv. Customer records to be located in any of:
 - A. Countries part of the high-risk third party countries list drawn up by FATF or the EU;
 - B. Countries in the high-risk countries subject to a call for action by FATF;
 - C. Countries which FATF considers to have strategic deficiencies.
- v. Countries which are under asset freeze and for which it is prohibited to make funds available;
- vi. Changes in the average deposit bands; and/or
- vii. Customers using Cryptocurrencies for deposits and withdrawals.
- viii. Customers using prepaid cards
- ix. Customers attempting to withdraw deposits which were not wagered
- x. Customers who do not provide the requested documentation
- xi. Individuals who do not provide identification details.

The risk profile may change due to product choice (game type), transaction pattern, transaction size, change in PEP status, hits on adverse media checks in the process of ongoing monitoring, and other risk variables, thus the customer risk assessment is carried out every 3 days and will determine whether there are any changes to the customer's risk rating. If there are any changes, this will be reflected in the risk rating which is shown in the customer profile.

6. Customer Due Diligence (CDD)

6.1 What is CDD?

CDD refers to the identification, verification and ongoing monitoring of a customer.

6.2 When is CDD Performed?

While identification is always performed on registration by collecting details on establishing the business relationship; by way of derogation for the gambling industry, verification could be performed when the customer reaches €2,000 in deposits. Notwithstanding, the Company applies a risk-based approach and should there be any suspicion that the gambling account may be used for reasons other than the purpose for which the gambling account is opened (i.e. playing online games of chance for leisure), verification is carried out prior to reaching the established deposit threshold.

6.3 How is CDD Performed?

6.3.1 Identification

The Company is required to collect details on the identity of all customers registering with it. To this end, the identification process of a customer is carried out upon registration. The Company does not accept anonymous accounts, accounts in fictitious names, duplicate accounts or accounts in the name of legal persons.

Customers are required to fill in the following details on registration:

- Email
- Password
- First Name;
- Last Name;
- Date of birth;

- Address;
- City;
- Postal Code;
- Country of residence;

For selected territories, the Company makes use of electronic means of identification (the deposit-and-play flow). In this onboarding flow, customers are required to input their electronic identification number (Bank-ID) to be able to register on to the Company's website instead of filling in the form established above. This electronic identification solution allows the Company to identify the customers by extracting the details associated with the electronic identification number and then saving them on the customer's gambling account on the back-office. Worth noting that, with a synchronous API call, the electronic identification number is run against the Company's database to ensure that no multiple accounts are created for the same customer. If no matches are found, a customer account is created on the Company's database. This step also ensures that the customer is not under the legal age.

For both means of identification, an automatic check through reputable third-party sources is conducted to scan for matches with PEP, sanction list, and adverse media databases.

6.3.2 Verification

a. Documentary verification

As a subject person, we are obliged to verify the details provided at registration when the customer reaches €2,000 in deposits on his gambling account. The documents requested are a government-issued identification document and a proof of address (for e.g. bank statement or a utility bill dated in the last three months). Identification documents accepted are:

- A valid passport
- A valid identity card
- A valid driving licence
- Travel documents for refugees and aliens
- Aliens' documents issued on the basis of the Aliens Act 2000

The documents are either uploaded on the account itself by the customer or received by our customer support on dedicated secure inboxes. The documents received are always made available on the customer's backoffice. The verification is carried out manually whereby, a designated team checks that the document is:

- Authentic - issued by a competent authority
- Valid - unaltered
- Current - not expired

and then matches the details on the document with the details on the account.

b. Electronic verification

In the case of registration via the deposit-and-play flow, verification of the customer's identity is carried out on registration. In that, the customer is not able to register unless they verify through such electronic means. With the use of a one-time code sent to the registering customer's mobile-phone number it is also affirmed, that the person whose details are being registered on the account, is the person actually opening the account.

6.3.3 Inability to Carry Out CDD

If the Company is unable to duly identify the customer, the business relationship is not established. On the other hand, if the Company is unable to verify the customer with whom it already has a business relationship, the CCompany may suspend the account until it could satisfactorily verify the customer or else terminate the business relationship. As part of ongoing monitoring of customers and aware that the customer's risk fluctuates, actions on the account may be taken on the customer's account depending on such fluctuations and the reasons therefore.

7. Enhanced Due Diligence (EDD)

7.1 What is EDD?

EDD is an extension of knowing the customer with whom a business relationship already exists. EDD may be required for various reasons as outlined below, however, in all cases, the intention is to obtain additional information and/or documentation in order to look into suspicious behaviour on the gambling account. Such suspicion may either raise questions about the identity of the customer himself and/or his source of wealth or the source of the funds of a particular transaction made on the account.

7.2 When is EDD Performed?

In line with the risk posed by the following events, the Company undertakes EDD on the following:

- i. Potentially sanction-listed individuals;
- ii. Potential adverse media matches;

- iii. Players subjected to suspicious activity reporting;
- iv. Players identified as top depositors if the activity is identified as irregular or suspicious
- v. Customers identified as top losers if the activity is identified as irregular or suspicious;
- vi. Customers for whom an internal suspicious activity report has been filed;
- vii. When customers register or log-in from a high-risk third country identified by FATF/EU Commission;
- viii. When players reach a certain net loss threshold;
- ix. When players have low wagering thresholds;
- x. Excessive use of prepaid cards;
- xi. Repetitive withdrawal requests without wagering high deposits;
- xii. Demographics elements such as player's nationality triggers for high-risk country together with other risk factors.

7.3 How is EDD Performed?

On the detection of a higher-risk trigger requiring EDD, the Company may opt to either, any or all of the following:

- Open sources
- Information from the customer
- Documentary sources requested from the customer
- Reports requested from third-parties

EDD is normally aimed at establishing the source of wealth of the customer and/or the source of funds of a specific transaction. These two EDD elements are elaborated upon below. Notwithstanding, it is also acknowledged that there might be other reasons for requesting EDD, for e.g. the CCompany requests a photo-holding ID when the pattern of gambling does not match the profile verified through simplified due diligence ('SDD').

7.4 Source of Wealth (SOW)

7.4.1 What is the Source of Wealth?

Source of wealth is the activity/activities (different sources) which generate the overall wealth of a customer, including but not limited to:

- i. Salaries
- ii. Bank savings
- iii. Selling a property
- iv. Inheritance payment
- v. Divorce settlement

The source of wealth provides an estimate of what may be the expected volume and value of transactions passing through the account held by the customer with the Company. While the Company is aware that it is not in a position to carry out a *forensic accounting exercise*, such information helps the Company to justify or otherwise the activity (namely in financial terms) on the gambling account. Since the scope of the source of wealth of an individual relates to that individual's net worth, proof of source of wealth is normally (but not exclusively) requested from customers who, accompanied by other red flags, are consistently high depositors and frequent players.

7.4.2 When is a Source of Wealth check performed?

The Company undertakes a source of wealth check when there is a suspicion as to the origin of the funds that are passing through the gambling account. The suspicion normally but not necessarily arises over a period of time.

7.4.3 How does the Company review SOW documentation?

Depending on the risk, the Company will opt to carry out SOW checks on the basis of any or all of the means established above. It is understood that at times, asking the customer for information may suffice to obtain information about the customer's source of wealth. This is done through a source-of-wealth form which the customer is requested to fill in to declare his source of wealth. Open sources, especially social media, helps backing up information provided by the customer without needing to request SOW documentation.

When documentation is deemed necessary, the AML team vets the document/s received for authenticity and validity. It is then considered in light of the transactions on the gambling account and, the level and nature of activity of the customer. In order to be able to justify the activity on the account, the source of wealth declared and attested for

by the customer must show that the customer could afford the spent recorded on the account. When this could not be duly justified, the business relationship with the customer is terminated.

7.5 Source of Funds (SOF)

7.5.1 What is the Source of Funds?

In contrast with the SOW, the SOF is narrower in scope, in that it relates to how the funds used for a particular transaction were obtained by the customer.

7.5.2 When is a Source of Funds Check Performed?

Over time, players establish a gambling profile with the Company. Such a profile is, amongst others, made up of the product that the customer predominantly plays on, the depositing pattern (amounts and frequency), and the level of activity on the account. Such gambling profiles vary from one player to another and therefore, the trigger for a source-of-funds check is specific to the gambling profile of the player. A source of funds check is deemed to be necessary whenever the gambling account registers a gambling transaction which diverges from that player's gambling profile. The Company gauges the level of risk attributed to that transaction on the basis of the divergence from the gambling profile. The further the divergence, the more rigorous the source-of-funds investigation is.

7.5.3 How does the Company review the Source of Funds?

It is to be noted, that at times, the source of funds could be justified by a mere review of the gambling account itself. For example, the customer may have just had a big win which would justify a sharp increase in his bet size; or the customer would have made a large withdrawal after a big win, and he then deposits some of it back on his gambling account, thus justifying, the higher deposit amount when compared to his normal depositing pattern. That being said, whenever proof of source-of-funds documentation is required, the Company requests such via email. The customer is requested to provide the origin of a particular transaction and this is normally obtained through a bank statement which would outline the date and origin of a certain amount of funds. In receiving SOF documentation, the AML team vets the document for validity and authenticity, and then proceeds to review it vis-a-vis the transaction in question. If the AML team is satisfied with the justification, the business relationship resumes, if not, the business relationship is terminated. There are cases, whereby, on receiving the

documentation, the source of funds is still not clear, in such cases, and on a risk-based approach, the AML team may either decide to suspend the business relationship or continue with it pending the receipt of further information.

7.5.4 Inability to obtain EDD

In case no EDD documents are received within an appropriate time frame, and the open-source searches and internal investigations do not produce enough proof to sustain the legitimacy and origin of the funds for a particular transaction and/or wealth of the customer, the matter is escalated to Head of AML and thereafter, the MLRO.

The non-compliance with a request for documentation triggers the internal reporting procedure/internal escalation as such customer behaviour is considered a reasonable ground for suspicion.

A decision is then made as to the action to be taken on the account and whether to proceed with escalating as a SAR/STR to the FIAU. If no escalation is made, then the reason for such a decision is documented.

7.5.5 Acceptable Documentation Guide

Table 1 outlines examples of source of wealth and/or source of funds documentation and information accepted.

Categories	Details Required	Additional Documents
Savings from employment income	Annual income and bonuses in the current and previous year. Nature of employer's business and employer's name and address if appropriate.	bank statements that clearly show receipt of the most recent 3 months. Regular salary payments from the named employer or latest accounts if self-employed.
Maturing investments or encashment claim	Date and amount received, from which entity and how long was the investment held.	Letter/contract note from previous investment entity providing notification of proceeds of maturing investment or claim.
Share sale	Description of shares/funds, how they were disposed of (i.e. through a stockbroker or bank etc. Including name/address), date of sale.	Legal sale document i.e. contract note. Bank statement showing sale transaction.
Property sale	Sale value of property sold, how it is sold (i.e. through agent, by auction, private sale, including name/address), date of sale.	Signed letter from solicitor or completed sale contract. Bank Statement or other document showing sale transaction.
Company sale or sale of an interest in a Company	Name and address of Company, total sale price, applicant's share, nature of business, date of sale.	Signed letter from solicitor or signed letter from regulated accountant or copy of contract of sale and sight of investment funds on bank statement.

Inheritance	Total amount received, date received, received from whom.	Grant of probate (with a copy of the will) which must include the value of the estate or bank statements or solicitor's letter.
Loan	Amount of loan, purpose of loan, name of lender, date of loan.	Loan agreement or recent loan statements.
Gift	Total amount, details of benefactor, reason for gift, relationship to benefactor, source of donated funds.	Letter from donor confirming details of gift and acknowledging the source of the donated funds. Based on the source of wealth specified the donor needs to provide supporting documentation as per the provisions in this matrix.
Company profits	Accountant giving details of Company profits over the last 2 years.	Financial Statements.
Other income sources	Nature of income, amount, date received, received from whom.	Appropriate supporting documentation or signed letter detailing funds from a regulated accountant.
Entrepreneurial (active)	Company name, short description of business, activities, place of business.	Website address and latest accounts.
Entrepreneurial (former)	Company name, short description of business/activities, place of business, year and details of sale of business.	Financial statement.

Table 2 - Examples of SOW and SOF documents accepted.

The purpose of these documents and information is to verify the affordability of the customer and the legitimate origin of the funds. Change of circumstances which trigger risk linked to the origin of wealth / funds, would require a re-assessment of the customer's wealth / funds.

8. Politically Exposed Persons (PEPs)

The Company does not currently have the risk appetite to maintain a business relationship with customers who are confirmed to be PEPs.

8.1 PEPs Individuation and Mitigation

Screening for PEPs, Sanctions and adverse media is carried out upon registration. This screening is carried out through a third party tool. Apart from triggering upon registration, the check is also carried out on a six monthly basis as part of the ongoing monitoring.

Whenever there are hits on the PEP, sanctions and/or adverse media databases, the details of the account are populated in a report which is extracted and reviewed on a daily basis by the AML team. During the review, the AML team first determines whether the hit is a false positive and in such a case, no further investigation is carried out. This is the case with the absolute majority of hits that we get on such screening.

When it transpires that the hit is genuine, and therefore, the match is confirmed, the business relationship is terminated and any deposits are refunded to the customer.

The team is able to trigger a PEP/sanctions check at any point in time, i.e. if details change or there is an event which would prompt another screening, then the customer is checked against the database without awaiting the routine check.

If a player becomes a PEP during the course of the business relationship, the Company will close the account immediately, reach out to the player, and request EDD to establish the source of wealth and determine legitimacy of gaming activity. .

9. Sanctioned Individuals

The Company screens individuals against the relevant data from each sanctions source which are included in the consolidated sanctions profile that the third-party provides. Examples of these are the UN Sanctions List, EU Sanctions List, OFAC List and the Russia Enforcement Sources.

Any customer which is flagged as a sanctioned person when his name is run against the sanctions register, will be vetted to determine the validity of the alert. If it transpires that the person is actually a sanctioned individual, the Company does not maintain a business relationship with the customer and the necessary reporting to authorities is carried out.

It is standard procedure to carry out ongoing monitoring whenever a request has been made from the stipulated authorities regarding new sanctioned individuals.

Whenever the sanction lists are updated, the particular list is matched against the Company's existing customer database to identify whether there are any sanctioned individuals in the customer database.

10. High Risk and Sanctioned Jurisdictions

The lists outlined below are included as part of the customer risk assessment methodology which means that when the risk assessment is carried out on the customer, his/her place of residency will influence the overall risk rating due to assessing the Geographical Risk. The Company is only onboarding players from reputable jurisdictions. To this end, the inherent geographical risk is significantly mitigated.

10.1 Directive (EU) 2015/849):

High risk third countries: (January 2022)

- Afghanistan
- Barbados
- Burkina Faso
- Botswana
- Cambodia
- Cayman Islands
- Democratic People's Republic of Korea
- Haiti
- Iran
- Jamaica

- Jordan
- Mali
- Morocco
- Myanmar
- Nicaragua
- Pakistan
- Panama
- The Philippines
- Syria
- Senegal
- South Sudan
- Trinidad and Tobago
- Uganda
- Vanuatu
- Yemen
- Zimbabwe

10.2 FATF: High- Risk countries subject to a call for Action October 2022:

- Democratic People's Republic of Korea (DPRK)
- Iran
- Myanmar

Source : <http://www.fatf-gafi.org/countries/#high-risk>

10.3 Jurisdictions considered by FATF with strategic deficiencies as updated in October 2022:

- Albania
- Barbados
- Burkina Faso
- Cambodia
- Cayman Islands
- Democratic Republic of Congo
- Gibraltar
- Haiti
- Jamaica
- Jordan
- Mali
- Morocco

- Mozambique
- Panama
- Philippines
- Senegal
- South Sudan
- Syria
- Tanzania
- Turkey
- Uganda
- United Arab Emirates
- Yemen

10.4 UN and EU sanctions:

Asset freeze and prohibition to make funds available:

- Afghanistan
- Central African Republic
- Eritrea
- Iraq
- Lebanon
- Mali
- Somalia
- Syria
- Yemen

10.5 OFAC sanctions:

[Specially Designated Nationals and blocked persons List](#)

11. Ongoing Monitoring

The Company is required to conduct ongoing monitoring of a business relationship, whereby this is applied on a risk-based approach. Ongoing monitoring entails the following:

- Scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions are consistent with the Company's knowledge of the customer and his/her business and risk profile; and

- Keeping the documents, data and information obtained for the purpose of applying CDD measures up to date.

The ongoing monitoring of transactions is being handled through various systems and checks integrated in the technical platform. The below are some examples of the tools that are used:

- Tailored Reports: These reports feed data directly from the databases where various parameters can be monitored, and patterns and/or deviant behaviour can be identified.
- Fraud rules: A series of advanced rules are set up to prevent players from using systems to circumvent our processes. The fraud tool is monitoring all financial transactions including gameplay, IP addresses, and device fingerprinting. The tool is also using real time data enrichment to build a more robust player identity profile.
- Risk score: An automated risk score is attached to each player which enables the Company to understand the player behaviour and model any future risks based on this score.
- Gameplay checks: Casino gameplay and sport bets are analysed by a specialised team that can identify that the gameplay and the random number generator are functioning as they should.
- Top Depositors report: A report including the top high rollers is extracted and analysed.

Periodical screening for existing players is to take place every 6 months, in the event of changes in circumstances (for example a player entering PEP status, or recent adverse media-findings)

The Company ensures that there is a high level of automation in the checks performed for ongoing monitoring thus ensuring that a sustainable, and realistic level of control is always upheld. A specialised and highly trained team of AML analysts apply ongoing manual monitoring on players that risk profile is set to a high level.

After any agent-led investigation by the AML Team, the Company might take one or more of the following actions based on the risk profile of the player:

- Disable some or all payment options for the player
- Reduce payment transaction limits for the player
- Request information on the source of funds
- Freeze funds in the player's account
- Cancel winnings and refund the deposits into the contra account

- Close the player's account
- Blacklist the player's IP address, device and/or payment account
- Revise the player's risk profile
- Report the player to the authorities

The Company does not:

- Send withdrawals to customers through payment methods that the customer has never used to make a deposit (not including bank account transfers and prepaid card deposits). During the withdrawal process, the Company verifies that the person who has deposited and has now requested withdrawal is the same person;
- Allow withdrawals to a different country than the country that the deposit was made; or
- Allow customer-to-customer internal payments (peer to peer payments).

12. Match Fixing

The Company, through its sportsbook provider and their odds/risks management capabilities, and its own investigations on raised suspicions, shall seek to mitigate risks associated with participants who directly or indirectly influence the outcome of a betting event, as well as third parties who, commissioned by these persons, place sports bets on the outcome or the course of the sports event, or promote sports betting by others.

The Company participates in an independent early warning system, which serves to defend against manipulation of the sporting competition and is suitable for identifying this at an early stage. Moreover, the Company understands that it is our obligation to inform the authorities immediately of any abnormalities, to participate in any clarification sessions held, and make available information. A suspicion of possible match fixing is, itself sufficient cause to presume that the transaction may be related to money laundering and thus must be reported to the relevant financial-crime authority.

13. Training

One of the most important controls over the prevention and detection of ML/TF is to have employees/persons within the Company who are alert to the risks of ML/TF, and who are well-trained in the identification of unusual activities or transactions which appear to be suspicious.

All senior management, and all employees/persons who are hired within player facing departments must undertake a mandatory training course in relation to AML/CTF within 180 days after the first date of engagement.

Training is provided upon the recruitment stage and on a yearly basis thereafter. The MLRO (or any person appointed by the MLRO) will also provide awareness sessions on an ongoing basis to serve as a refresher.

The objectives of the training courses are to:

- Understand the age verification and KYC processes and procedures;
- Understand the basics of money laundering and funding of terrorism;
- Know the AML/CTF laws applicable;
- Understand their responsibilities for the prevention of money laundering and terrorist financing;
- Understand the money laundering and terrorist financing risks faced by the Company and appreciate the need for customer due diligence;
- Recognize the red flags for ML/TF and appreciate the need for suspicious activity reporting; and
- Understand the procedures for reporting.

Employees are also trained internally to understand and be aware of:

- Company's procedures for managing money laundering and funding of terrorism risks;
- The identity, role, and responsibilities of the MLRO, and what should be done in his/her absence;
- How CDD is undertaken;
- How customers are monitored when verification is not successful upon online registration; and
- How PEPs are identified.

The Company monitors the effectiveness of such training sessions to ensure that all employees/persons are trained in an appropriate and timely manner, and the training is fit for purpose.

14. Supporting Records Retention Period

For the purposes of the record keeping requirements the Company retains the drop/win figures for each named customer for at least 5 years.

15. Review

This Policy is reviewed every two years or whenever there are changes to the Company's operations which need to reflect its content.