

**Anti-money Laundering, Combating the Financing of
Terrorism and Proliferation of Weapons of Mass
Destruction (AML/CFT/CFP) Policy**

GALAKTIKA N.V.

Scharlooweg 39 Willemstad, Curaçao

May 2025

Document Information

Subject	AML/CFT/CFP Policy
Purpose	Company procedures for Anti-Money Laundering, Fraud and Payments ongoing tasks
Involvements	All departments
Responsibility	MLRO
Approval	Director
Review	Annually or earlier as needed
Classification	Company Confidential
Version	2.1
Updated By	MLRO
Authorised By	Director
Distribution Date	20/05/2025

1 Introduction/Policy statement

“Money laundering” is generally defined as “engaging in acts designed to conceal or disguise the nature, control, or true origin of criminally derived proceeds so that those proceeds appear to have been derived from legitimate activities or origins or otherwise constitute legitimate assets.”

“Terrorist Financing” is the financing of terrorist acts, of terrorists and terrorist organizations. A terrorist act is an act to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act. The money involved in a terrorist financing act is not necessarily derived from illicit proceeds

“Financing of Proliferation of weapons of mass destruction” is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

The Proceeds of Crime are funds derived from illicit sources and from which a benefit or enjoyment may be obtained. Although the aim is not to launder the funds or to fund terrorism or proliferation, it is still considered to be an illegal activity and subject persons should be aware of such activity and must report it as if it was ML/FT//FP.

The policies set forth herein (the “Policies”) are intended to satisfy the statutory requirements of the relevant legislation and to provide direction to GALAKTIKA N.V. (or “the Company”) in complying with its obligations at law by taking all reasonable steps and exercising all due diligence to avoid the commission of an offence of money laundering or funding of terrorism.

The Company is aware that criminals and terrorists may attempt to use the Company’s services to channel funds from illegal activities.

In conducting its activities, the Company complies with the following Curaçao laws and regulations, as mentioned in Appendix 1, that govern anti-money laundering (AML), counter-terrorist financing (CFT), and counter-proliferation of weapons of mass destruction (CFP):

- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92);
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators
 - as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
 - Sanctions National Ordinance (N.G. 2014, no. 55);
 - Kingdom Sanction Act (N.G. 2016, no. 54);
 - National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
 - National decree for general measures, of the 10th of July 2015, for the implementation of Article 2 of the sanctions National Ordinance, containing implementation of the United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
 - National Decree for general measures, of the 10th of July 2015, for the implementation article 2 of the Sanctions National Decree containing implementation of the of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
 - National Decree for general measures, of the 10th of July 2015, for the implementation of
 - Article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30)
 - National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34)
 - The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48)

In addition, the Company follows sanction regimes established by the UN (United Nations), the EU (European Union), and the US OFAC (Office of Foreign Assets Control) when identifying and blocking sanctioned persons or entities. These laws and regulations define the Company's obligations to identify clients, monitor transactions, apply freezing measures (if warranted), and so forth.

The Company shall review AML/CFT effectiveness within the Company, to ensure that the AML/CFT policies and procedures are being respected within the business and to identify any gaps in controls that may need to be addressed. The Company's internal audit function (IAF) will be responsible for the review as approved by the Audit Committee / Director. The terms of appointment to the IAF will include clear and explicit provisions of the respect to confidentiality and non-disclosure in relation to sensitive data that they might come across during the review.

Scope of the Policy

The scope of this policy is to establish Policies from which procedures on internal control, risk assessment, risk management and compliance in relation to AML/CFT/CFP will be drawn up.

Users of this and related policies should also refer, where relevant, to the Applicable Laws and any other relevant measures/guidelines which may be issued from time to time by the Financial Action Task Force ("FATF") and/or any relevant authority or agency.

Unless the context requires otherwise, words and expressions used in the Policies shall have the same meaning as that set out in the applicable laws and regulations.

The Company is determined and committed to prevent the carrying out of financial activities through its systems that may be related to ML/FT/FP.

The Company shall comply with its obligations at law by establishing the necessary and relevant processes to prevent ML/TF/FP and to ensure any suspicious activities are escalated to the relevant authorities.

The Policies outline the general and minimum standards of internal anti-money laundering, combating the financing of terrorism and the financing of proliferation of weapons of mass destruction (AML/CFT/CFP) Policies which should be adhered to by the Company's management and employees.

1. Risk Assessment

The basis of the risk-based approach is the risk assessment which need to be carried out to understand and identify the ML/TF/PF risks the business is exposed to and to ensure that policies, controls and procedures exists to mitigate those risks.

1.1. Business ML/TF/PF Risk

The Company is to carry out a yearly risk assessment to identify the ML/TF/PF risks the Company is exposed to and ensure that the policies, controls and procedures adopted are adequate to prevent and mitigate those risk. The Business Risk Assessment will identify the following risks:

- identify ML/TF/PF Vulnerabilities;
- identify ML/TF/PF Threats; and
- identify any new requirements.

Based on the results of the Business ML/TF/PF Risk Assessment and if deemed necessary, in order to minimize any new risks identified or existing risks being re-classified, the following controls would need to be revisited and amended accordingly:

- measures;
- policies;
- controls; and
- procedures.

The Business ML/TF/PF Risk Assessment should be monitored and improved whenever substantial changes to the Company's systems, processes, new markets, new games, regulatory changes and overall operations.

The Business ML/TF/PF Risk Assessment and related measures, policies, controls and procedures are to be recorded and made readily available for review by the interested authorities at any time.

1.2. Customer ML/TF/PF Risk

As each customer exposes the Company to different risks, a player-specific risk assessment must be carried out so the Company is able to identify the potential risks it faces when entering into a business relationship with, or carrying out an occasional transaction for a player. The customers risk assessment is based on:

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

The assessment enables the Company to develop a risk profile for the customer and to categorize the ML/TF/PF risk posed by such player/customer as low, medium or high.

After registration, a customer's activity will undergo ongoing monitoring through automatic and manual processes to reconsider risk level depending on changes in customer's activity and to establish the point of reaching the relevant due diligence requirements thresholds.

1. The customer risk assessment – an ongoing process

Customers registering for the Company's services are normally considered to have registered to make use of the Company's remote gaming services for recreational purposes. Therefore a "normal" customer will not be automatically suspected to have registered to carry out money laundering or financing of terrorism.

Blind faith, however, is not to be exercised and instead, the Company must carry out a range of ongoing checks and monitoring to ensure that a customer's activity is legitimate. This is carried out by risk assessing customers for the risks of money laundering and financing of terrorism.

A customer's money laundering and financing of terrorism and proliferation risk assessment is to be performed at all stages of a customer's relationship, from registration to closure. In line with the risk-based approach as mandated by the relevant laws, regulations and guidelines in force, the customer risk assessment is re-visited regularly during the customer's interactions.

Therefore, when customers use the Company's services, profile information, actions performed on the account such as deposits, placement of bets, withdrawals and any other information obtained from the interactions with the customer or from third parties in relation with the customer are assessed to identify whether the customer's risk assessment needs to be reconsidered. This is an ongoing process.

This policy outlines several procedures designed to identify, verify, and assess customers at key points in their relationship with the Company. It also covers additional procedures such as Sanctions and PEP Screening, Customer Due Diligence, and Suspicious Transaction Reporting, which collectively help mitigate and manage ML/TF/PF risk.

1.1. Risk levels

The customer's risk assessment will enable a risk profile to be developed in assigning one of three levels of risk to a customer.

The Company applies risk-based approach (hereinafter – "RBA") that entails:

- Recognising the existence of risk(s);
- Undertaking an assessment of the risk(s):
 - geographical areas of operation;
 - customers and any underlying beneficial owners;
 - products or services;
 - transactions;
- Developing strategies to manage and mitigate the identified risks;
- Monitoring and identifying ways for improvement of risk-mitigating measures;
- Keeping records of undertaken actions and underlying reasons.

The core objectives of the Company while following with the RBA obligations are:

- Identify and assess the risks of money laundering and terrorist financing to which the Company's business is subject;
- Appropriate systems and controls must reflect the degree of risk associated with the business and its customers;

- Determine appropriate CDD measures on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction;
- Take into account situations and products which by their nature can present a higher risk of money laundering or terrorist financing; these specifically include correspondent banking relationships; and business relationships and occasional transactions with PEPs.

The risk assessments carried out must be documented, kept up to date and made available to FCA upon request.

For the identification of risk level to which the Company is susceptible the Company has adopted criteria consisting of four risks:

1) Geographical. The geographical risk factor establishes the risk score of a particular country which is further used for the assessment of the risk score of either customer or transaction.

The Company considers the following whenever deciding on the geographical risk score:

- Countries on the FATF list of High - Risk Jurisdictions subject to a Call for Action;
- Countries on the FATF list of Jurisdictions under Increased Monitoring;
- Countries on the CFATF Public Statement;
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);
- Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;
- Countries sanctioned by the OFAC;
- Countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International.

It should be noted that no countries have zero risks for money laundering, some of them, of course, have a lower risk. Even beyond that, many low-risk countries have issues that need to be addressed, for example, related to beneficial ownership or politically exposed persons. Countries are assessed on a case by case basis and the Company will remain cautious at all times of any shortcomings that are present within a particular jurisdiction.

The Company considers the risk posed by the geographical location of the business/economic activity and the source and destination of funds of the customer the location of the financial institution sending/receiving, as well as the nationality, residence, citizenship, and place of birth of a customer. Notably, countries with EU equivalent AML/CFT regimes could pose a lower risk. At the same time, some jurisdictions may pose a higher risk by virtue of common trading such as drug trafficking and terrorism.

As a basis for the risk scoring matrix, comprising 245 countries, the Company is using "Know Your Country"-scoring model. The "KnowYourCountry" rating assigned to a country represents a collection of independent indicators that together represent a total score assigned to a particular country. The table below outlines the factors and their weight for the total score as is initially assigned by "Know Your Country":

Indicator/ Sub Indicator	Weighting
1. Money laundering/terrorist financing risks	56
1.1. FATF Uncooperative / AML Deficient	25
1.2. FATF Compliance with MER rec assessments	10
1.3. US State ML Assessment	15

Document Classification: Company Confidential

1.4. US Secretary of State terrorism	6
2. International sanctions	15
3. Corruption risks	10
4. World Governance Indicators	3
5. Narcotics Major List	3
6. Human Trafficking	3
7. EU Tax Blacklist	5
8. Offshore Financial Center	5
Total Available Score:	100

The overview of the scores in the matrix is in Annex 7. Notably, for the purposes of assessing the risk score, the numbers provided by «Know Your Country» are reversed as they reveal compliance with the indicators stated above. The Company does not blindly follow scores identified by the Annex 7 and where relevant it adjusts scores in order to represent the risks presented by the countries as seen from the perspective of the Company, it is the responsibility of the MLRO to assign risk scores to the countries.

The MLRO is responsible for keeping this matrix up-to-date and will perform a planned review at least each third month. The MLRO will keep under review publications by relevant bodies and in accordance with such review will perform adjustments to the scores assigned to a particular jurisdiction. In cases where unexpected circumstances that should be reflected in the score of the country occur, the MLRO will perform an occasional review of the matrix and make corresponding changes. The non-exhaustive list of the sources which will be used for such purpose is as follows:

- Office of Financial Sanctions Implementation (OFSI); (<https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets>);
- The country assessment reports prepared by the FATF (<http://www.fatf-gafi.org>);
- MONEYVAL Committee of the Council of Europe (www.coe.int/moneyval);
- EU Common Foreign & Security Policy (<https://eur-lex.europa.eu>);
- UN Security Council Sanctions Committees (www.un.org/sc/committees/);
- International Money Laundering Information Network (IMOLIN) – (www.imolin.org);
- International Monetary Fund (www.imf.org);
- Transparency International (<https://www.transparency.org>).

2) Customer type. Customer risk is the risk of ML/TF that arises from maintaining relations with a given person. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. Categories of customers whose activities may indicate a higher risk include:

- Customers who have multiple sources of income;
- Customers with irregular income streams;
- PEPs;
- High spenders (money can be derived from illegal activities);
- Disproportionate spenders (inconsistent with casino's information about customer's known source of income/assets);
- Casual customers like locals/tourists, especially when spending pattern changes;
- Improper use of third parties, criminals use third parties to gamble to break up large amount of cash, to buy chips or to cash out on behalf of others to avoid CDD measures;
- Multiple casino player rating accounts to hinder a casino to track their gambling activities;
- Unknown customers (redeeming large amounts of chips);

- Junkets (junket operators monitor player activity and issues and collect credit).

There are also "prohibited" type of customer risk attributes:

- Sanctioned individual or entity;
- Anyone deemed to be linked with the financing of terrorism;
- The Company shareholder;
- Closed jurisdiction customer location;
- Source of funds/wealth – cash or funds appear to be generated or linked to the proceeds of crime.

3) Products and services. Some **products** or services are inherently riskier than others and are therefore more attractive to criminals. These include products or services which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the customer to influence the outcome of a game, be it individually or in collusion with others. The use by customers and the acceptance by casinos of specific payment methods, which are considered to present a higher risk of ML/FT, should also be treated as high risk factors. The risk level of the products/services is set out in Annex 6.

4) Distribution channels.

While evaluating the risk presented in a particular case, the Company ensures that the associated risk score is not unduly influenced by whichever one factor. All of the factors which are presented above are used cumulatively in a formula that calculates an overall risk score for a particular case. They differ whenever an assessment is undergoing for: geographical risk score, customer risk score, product/service risk score, transaction risk score. Therefore, it may happen that even in cases where the overall risk score of the customer is low the relationship will not proceed or will be terminated at the onset as a consequence of customer revealing higher than the acceptable level of risk in one particular risk factor. As well, the Company ensures that the employed formulas are not unduly arranged as to prevent the customers from falling within the higher risk.

The formulas which are used for each particular case will be further revealed and practical application will be considered while outlining each risk factor. Notably, the risk score which is determined may be amended at whichever time by the MLRO of the Company regardless of the calculation presented by the formulas. The MLRO may at any time determine that whichever customer or transaction is unacceptable as a consequence of independent evaluation.

The Company has established fractured differentiation of the risk scoring and identified 4 levels of risk. A risk rating simplifies the process of collecting a vast variety of potential sources of information and usually aggregates a number of variables into one comprehensive score helping to determine the risk level of a particular case.

The total risk scoring will represent 4 different risk levels per which particular action will be undertaken in regard to the customer/transaction falling within a certain risk level. The table below outlines who should take decisions regarding particular customer/transaction, what kind of review should be carried out, how often the annual review on the viability of relationship should be undertaken, and ways of actions in accordance with the risk level at hand.

Total Risk Scoring	1-19	20-39	40-49	50<
Risk Level	Low	Medium	High	Prohibited
Due Diligence	CDD	CDD/EDD	EDD	N/A
Approval	MLRO	MLRO	MLRO	N/A
Monitoring	Annual review by MLRO	Annual review by MLRO	Semi-annual review by MLRO	N/A

The table above illustrates that the Company will only deal with the first three risk levels (i.e. Low Risk, Medium Risk, High Risk). The Company shall not enter into a relationship with anyone who falls within the Prohibited Risk.

The risk scores range from 0 to 100 and are based on a progressive model - the higher the score the more risk is presented. Such an approach is taken in order to represent in plain terms the evaluation of risk which is carried out.

In order to calculate the total risk level of red, amber and green, the probability and impact relationship levels are assessed in relation to each other. This determine the correct proportionality for the control measures, which need to be put in place. This is sometimes referred to as the 'inherent risk' – the risk that resides in the essential nature of a product, feature, payment method characteristic etc., which must be addressed to avoid that risk materialising and/or to mitigate the effect of that materialisation. The table below demonstrates how the Company arrived at risk assessment and the red/amber/green determination.

PROBABILITY	Highly Likely					
	Likely					
	Possible					
	Unlikely					
	Highly Unlikely					
	Risk Eliminated					
		Insignificant	Minor	Moderate	Major	Severe
		IMPACT				

These levels will be defined as stated, but one must keep in mind that there will always be cases that may not fit into one specific range, as each player/customer may exposed the Company to different risk. In such cases, a cautious approach should be taken, and additional due diligence and/or consultation should be carried out with supervisors or the MLRO to ensure the assessed risk level of a customer is appropriate.

The factors inherent to the Company's clients, which may indicate varying risk levels based on the type of clients and their characteristics, are outlined in Annex 5. In addition, the three categories of players, based on their risk levels, have the following attributes:

1.2.1. Low risk customer attributes:

- Customer registered from a country not considered to have a high risk of money laundering, terrorist financing, corruption, fraud and having completed registration with plausible identification details and complete profile information;
- Customer passed registration procedure and provided the Company with at least the contact e-mail or phone as applicable;
- Has deposited less than XCG. 4,000 (€2000) (all amounts hereinafter are indicated in XCG., approximate EUR equivalents are provided for simplification and rounding purposes only, based on publicly available exchange rate information, in the event of any currency fluctuations, XCG. shall prevail for calculation purposes) in the last six months for low risk payment methods or less than XCG. 2,000 (€1,000) from low-medium risk payment methods in staggered deposits (refer to Annex No. 4);
- Customers using a limited number of payment methods which are in the customer's name;
- Placed reasonable bets on the Company's remote gaming products in line with "normal" gaming activity seen from regular customers with the same registration country or funding patterns;

- Effect closed-loop withdrawals whereby the withdrawals are requested to the same payment method from which those funds originate and are not substantially higher than those deposited by the customer;
- Customer has completed Customer Due Diligence successfully.

1.2.2. Medium risk customer attributes:

- Customers with valid-looking registrations who register from unusual countries not targeted by the Company but that are not countries with high risks of money laundering, terrorist financing, corruption, fraud, etc;
- Customers who reach the threshold XCG. 4,000 (€2000) in deposits within the previous 6 months using low risk payment methods or XCG. 2,000 (€1,000) in deposits within the previous 6 months using low to medium risk payment methods;
- Customers whose Gaming activity is above average for a similar playing customer but not alarming;
- Customers who request withdrawals to a different payment method due to payment method inability to receive withdrawals which has been confirmed to be true.

1.2.3. High risk customer attributes:

- Customers with invalid or suspicious registration details / origin IP address not matching customer country, verification of e-mail or phone not performed;
- "Identity theft" category of customers;
- Customers trying to have multiple accounts registered;
- Customer account used from multiple locations within an unreasonable timeframe or change of pattern from normal usage;
- Customer identified as a Politically Exposed Person or listed on a Sanction List;
- Customer deposits using third party payment methods or uses high risk payment methods such as quasi-cash payment methods;
- Customers that deposit unreasonable amounts in relation to their Gaming activity or when they would still have funds within their account which were available for Gaming;
- Customers who have deposited more than XCG. 20,000 (€10,000) over the previous year and have not yet provided basic source of wealth information;
- Customers whose Gaming activity is beyond expected Gaming behaviour in relation to similar players and own funding sources or wealth (i.e. customers often changing their spending patterns);
- Customers who demonstrate signs of problem gambling;
- Customers who request withdrawals to alternate payment methods rather than to origin of customer funds or request withdrawals to third party payment methods;
- Customers who refuse to provide due diligence documentation, or provide invalid or fake documentation;
- Customers who refuse to explain unusual or suspicious access or who do not sufficiently explain unusual or suspicious activity on the remote gaming system;
- Customers flagged by payment providers, verification providers, law enforcement bodies or other industry collaborative platforms as potentially suspect customers or engaging in fraud, money laundering, terrorist financing etc.
- Customers who have multiple sources of income;
- Customers with irregular income streams;
- High spenders (money can be derived from illegal activities);
- Disproportionate spenders (inconsistent with casino's information about customer's known source of income/assets);
- Improper use of third parties, where criminals use third parties to gamble to break up large amounts of cash, to buy chips, or to cash out on behalf of others to avoid CDD measures.

2. Customer Due Diligence

Based on the requirements of various statutory obligations, including applicable laws issued by the Curaçao Gaming Authority, the Company is prohibited from keeping anonymous accounts or accounts in obviously fictitious names.

The Company must identify the player and ask for the player's name and other relevant information to determine the purpose and nature of the business relationship. Without sufficient knowledge, the Company may not establish or maintain a business relationship or carry out occasional transactions. A Customer Due Diligence program is the best way to prevent money laundering, financing of terrorism and financing of proliferation.

Customer Due Diligence measures are to be undertaken when:

- a. players engage in financial transactions equal to or above XCG. 4,000 (€2,000);
- b. carrying out occasional transactions above the monetary equivalent of XCG. 4,000 (€2,000);
- c. there is a suspicion of money laundering or terrorist financing; or
- d. the Company has doubts about the veracity or adequacy of previously obtained customer identification data.

A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount in excess of the monetary equivalent of XCG. 4,000 (€2,000).

Transactions are considered as linked if for example they are carried out by the same player through the same game or in one gaming session. In this case it would be expected to apply additional CDD measures. In this context, the Company has to identify the player, carry out a customer risk assessment and verify the identity of the player.

Whenever an occasional transaction presents a high risk of ML/TF, the enhanced due diligence measures must be applied.

Customer Due Diligence (CDD) Measures include:

- collection of identification details;
- verifying the identity of the customer;
- determining the customer profile and levels of activity and adjusting the profile as and when necessary;
- conducting ongoing monitoring of the business relationship, to ensure transactions are consistent with what the business knows about the customer, and the results of the risk assessment; and
- retention of records of these checks and update them when there are changes.

The CDD Procedure defines the procedure used to carry out CDD including timeframes when this will be triggered and in which cases Enhanced Due Diligence will need to be performed.

Depending on the customer's risk profile, customers who have been requested to complete the CDD Procedure may have their account restricted during this period.

Should the CDD Procedure not be completed within the established timeframes of such a request, the customer's account will be considered to have failed completing CDD and thus will be denied from any further activity. The raising of a Suspicious Transaction Report (STR) is to be considered. Such a decision is to be taken and recorded by the MLRO.

Unless a STR has been raised and an appropriate period has passed in which the customer has still not completed CDD, the account may be closed, and deposited funds still present on the customer's account will be returned to the deposit method, where possible, less any charges incurred by the business for transmission to this destination.

2.1. Identification and verification of the player

Identification refers to the collection of personal details of the player to establish the identity of the player.

2.2. Registration/Identification form

For a customer to register an account/pass the identification procedure, the following information can be collected:

- i. Name and Surname;
- ii. Date and Place of Birth;
- iii. Residential Address and Postal Code;
- iv. Gender;
- v. Nationality;
- vi. National Identification Number (if applicable);
- vii. Contact number (Mobile);
- viii. E-mail address;
- ix. Currency selection;
- x. Politically Exposed Person (PEP) Status Declaration;
- xi. Username required;
- xii. Password requested;
- xiii. IP Address & IP Country;
- xiv. Device Information (Browser and OS Version);
- xv. Cookie Reference data;
- xvi. Referring Link (if any) and/or Affiliate.

Notes:

1) However, in low risk scenarios the Company may limit information to be collected to the three personal details set out in (i) to (iii) above. On the other hand, in high risk situations, it is possible that the Company considers the collection of additional personal details as necessary to mitigate the higher risk of AML/CFT/CFP.

2) Registration will not be allowed to proceed unless the customer's registered Date of Birth indicates that the customer is older than 18 years of age. In the case the customer's age is younger, the customer's registration would be refused, and the customer served with an opportunity to contact support.

3) If IP address is identified as being different from origin country, a known potential proxy, or from a high-risk country as identified in the Geographical Risk Matrix (Annex 7), a generic refusal to accept registration will be served with opportunity to contact support.

2.3. Basic validation and multiple account checks

Once customer has completed the initial registration form, the customer is requested to complete verification procedure by completing the following:

- provide a personal verification code sent by e-mail to his registered e-mail address;
- click a link in the same verification e-mail which would automate the entry of the verification code.

In cases where a customer's registration matches higher risk criteria, such as use of promotional codes or from countries considered as portraying a higher risk of fraud, the following registration conditions may also be enforced prior to continue the registration process:

- enter a code received by SMS message to his registered mobile phone number, or
- enter a code using a two-factor authentication system (e.g. Google Authenticator).

Once account opening validation is confirmed, the system will check for likelihood of multiple registrations based on customer details and IP Address captured on registration & validation stages.

If no relatively similar accounts are found, account status will be set to “Active” and customer will be served a confirmation page. Customer will as part of the confirmation page be provided with:

- the ability to set expected spending profile;
- information about how to set limits to his account; and
- an option to upload identity verification documents for identity verification and to provide in advance copies of payment methods to be used.

Verification can be carried out by making reference to an unexpired government-issued document containing photographic evidence of the customer’s identity (e.g. passport, identity card). Where such a document does not allow verification of the customer residential address, the Company can obtain other documents like a bank statement, utility bill, letter from a public authority or rental agreement, which should not be more than six months old to verify the residential address.

The Company can also contact the player by letter, e-mail or telephone to verify the information supplied as well as send a verification code to the e-mail address to verify that the address is current and genuine. Verification can also be done by checking social media, telephone directories, companies registries or media and news sources.

Biometric checks can also be used to confirm that the customer-individual providing the document is the one described therein. There are also circumstances in which the Company is able to cross reference the information in his possession with geo-location information, IP address data, funding method data etc.

If the multiple registrations check has identified potential duplicate account matches, and depending on the criteria matching level, the customer will be served instead with:

- either a refusal of registration due to duplicate account (refer to Annex 3) or;
- successful registration page as above but at the same time the account is flagged for further detailed checking by Management.

2.4. High-risk client checks

Customers who have been identified to be potentially high-risk clients, are to be recorded in the “High-risk Client Monitoring Spreadsheet” saved in the network folder assigned to the MLRO. This file is to be password protected and be accessible to the least number of employees as possible (and be recorded as such) as long as it includes at least two persons, one of them being the MLRO.

On a weekly basis, the customers in this list are to be checked and the risk level re-assessed (either as a stand-alone task or during other checks). The Spreadsheet template as set needs to be maintained and appropriate notes filled in on each customer spreadsheet with a log indicating the activity which has been observed and any further actions taken.

If a customer triggers any suspected ML/FT/FP activity, an Internal STR Report should be raised as per the Internal Suspicious Transaction Report (STR) Procedure. No specific note should be left in the CMS but in the “High Risk Client Monitoring Spreadsheet”.

The Company also applies a Targeted Financial Sanctions (TFS) policy consistent with the Sanctions National Ordinance (N.G. 2014, no. 55) and international sanctions programs (OFAC, EU, UN). Specifically:

- (i) If at any point a client, or a related person/entity, is found on any applicable sanctions list, the Company will immediately freeze all of that client’s accounts and assets.

- (ii) The MLRO must be notified promptly, and where necessary, the regulatory authorities or the FIU will be informed.
- (iii) It is strictly prohibited to tip off the client or any other party that such freezing or investigation actions are underway.
- (iv) Account reactivation or release of funds can only occur if it is confirmed that sanctions provisions are not being breached, and with explicit approval from the MLRO.

2.5. Enhanced due diligence

The Enhanced Due Diligence (EDD) measures should be consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual. Enhanced Due Diligence has to be conducted where the risks of money laundering or terrorist financing are higher.

This concerns for example:

- Residents of higher risk geographic areas;
- Political Exposed Persons (PEP's);
- Products or transactions that might favor anonymity;
- New products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

The applied measures must be consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of Enhanced Due Diligence measures include:

- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the source of funds or source of wealth of the player.

Examples of source of funds include personal savings, employment, pension releases, share sales and dividends, property sales, gambling winnings, inheritances and gifts and compensation from legal rulings;

- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship;
- Conducting enhanced monitoring of the business relationship;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards;
- Other measures, including those necessary ensuring compliance with applicable laws and international best practices.

In situations presenting a higher risk of ML/TF, source of funds information has to be requested from time to time even though there may not be any change in pattern or activity conducted by the customer. For crypto-related payments, Enhanced Due Diligence may include verification of the origin wallet, source of crypto assets, and identity of the wallet owner. The Company may request blockchain transaction report, wallet explorer links, or third-party confirmations.

2.6. PEP / Sanction List checking

All players are screened against sanctions lists of the UN and EU. If Curaçao publishes a local list with designated persons and organizations, the Company also takes that local list into account. The Company does not do business with customers that are subject to international sanctions. Should a customer declare to hold a PEP status at registration, or otherwise, at the first deposit attempt, customers are checked to confirm whether the customer

is or is a family member or known associate to a person that is considered a PEP or is listed on a Sanctions List.

Before interacting for the first time with a customer, the Company checking published lists of known or suspected terrorists or other sanctioned persons or companies, such as but not limited:

- U.S. Treasury's Office of Foreign Assets Control's (Specially Designated Nationals and Blocked Persons List Specially Designated Nationals And Blocked Persons List (SDN) Human Readable Lists | Office of Foreign Assets Control (treasury.gov));
- EU Sanctions List (<http://www.sanctionsmap.eu/#/main>).

For PEP status screening the Company can also rely on internet search or consult reports and databases on corruption risk, like but not limited the Transparency International Corruption Perceptions Index or on www.knowyourcountry.com. Customers matching one of these are automatically flagged as "High Risk".

PEP's are considered as clients that pose a "High Risk" to the Company and as such warrant the implementation of Enhanced Due Diligence. Enhanced Due Diligence measures include, but are not limited to:

- Taking reasonable measures to establish the source of wealth and the source of funds. The investigation must then determine whether the PEP's spending pattern matches his legal source of funds. The Company requests a statement from the PEP about the source of funds and verifies them by consulting independent and reliable sources;
- Carrying out additional searches (e.g., internet searches using independent and open sources) to better inform the customer risk profile;
- Undertaking further verification procedures on the customer or beneficial owner to better understand the risk that the customer or beneficial owner may be involved in criminal activity;
- Verification of submitted certified documents by e.g., contacting the certifier;
- Ensuring that the identification documents of its high-risk categories of customers and beneficial owners are updated more regularly;
- Undertaking regular reviews of customers to detect if an existing customer may have become a PEP;
- Continuous monitoring of PEPs who hold prominent public functions domestically or internationally;
- Increase awareness of higher-risk clients and transactions across all departments of the trust service provider that service this client;
- Increasing the frequency and intensity of transaction monitoring;
- Other measures, whether directly or indirectly referred to in Clause 2.6 or any other clause, as well as those necessary ensuring compliance with applicable laws and international best practices.

2.7. Gaming winners / losers

On a daily basis, a summary is extracted from the CMS showing the top winners and losers for the previous day, week, month and lifetime. Data fields amongst others will include platforms, specific and unspecific game or markets, numbers of bets, profit & loss, return to player percentages, customers total deposits and withdrawals, number of payment methods and any other information deemed relevant for this control.

Customer accounts on this summary are to be analysed for:

- Unreasonable losses or wins;
- Fraudulent use of payment methods;
- Irregular activity or potential Gaming cheats;
- Exploits of system issues; and,
- Customers exhibiting potential responsible gaming issues.

Where the Company employees suspect that the Gaming activity indicates potential cases of match fixing and/or other illegal activity, this must be reported through an STR in line with the Internal Suspicious Transaction Report (STR) Procedure.

3. Payment Methods

The Company will not accept to receive or make cash deposits or payments in relation to customer's activities.

The Company will only make use of payment methods that are:

- offered by licensed financial institutions and regulated by financial regulator; and
- if integrated through payment service providers, these would have been approved.

The Company will hold received payments from customers into a player's account, distinct from Company accounts.

The Company will always keep track of transactions carried out using these payment methods and identify funds that are received or remitted by customers, together with any transfers of funds that are made into or out of the player's account for settling the customer's remote gaming activity. It will also be able to identify when thresholds for CDD have been reached.

In all instances, where possible, funds returned to customers shall be returned to the customer's originating payment method. If this is not possible due to the nature of the payment method or in case of the account not being available any more to receive funds, payments will be transferred only to the bank account in the customer's name, following the completion of the CDD process.

4. Suspicious Transaction Report

An internal Suspicious Transaction Report is to be sent directly to the MLRO whenever there is a suspicion that a customer is engaged in ML/TF/PF.

No one is to divulge to co-workers, line managers and especially the customer/s that an STR has been raised as this is potentially considered to be 'tipping-off'. An employee who raises an STR must escalate directly to the MLRO.

5. Money Laundering Reporting Officer (MLRO)

Within the Company's internal control framework, there key role for AML/CFT/CFP compliance - the Money Laundering Reporting Officer (MLRO). MLRO responsibilities shall include but are not limited to:

- Develop and update internal policies and procedures on AML/CFT/CFP.
- Monitor and test the effectiveness of these procedures on an ongoing basis.
- Prepare and submit annual AML/CFT/CFP compliance reports to senior management.
- Analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions.
- Review all internally reported unusual transactions for their completeness and accuracy against other sources.
- Keep records of internally and externally reported unusual transactions.
- Design an internal procedure specifying when the reporting of unusual transactions will lead to blocking/freezing of user accounts, taking into account the risk of tipping off the player, and conduct closer investigations of unusual transactions if necessary.
- Prepare external reports of unusual transactions, receiving and evaluating all internal Suspicious Transaction Reports (STRs).

Document Classification: Company Confidential

- Liaise with the Financial Intelligence Unit (FIU) and law enforcement agencies.
- Decide whether to file external Suspicious Transaction Reports (STR) or Suspicious Activity Reports (SAR).
- Design, implement and update the AML program.
- Ensure customer due diligence measures and ongoing monitoring.
- Maintain records, including those related to internally and externally reported unusual transactions.
- Execute internal control procedures.
- Perform internal auditing of AML/CFT/CFP processes (unless a dedicated internal auditing function is available).
- Monitor and manage compliance with, and the internal communication of, such policies and procedures.
- Monitor relevant staff and agent screening processes.
- Conduct self-education and ensure the education of relevant staff in AML/CFT/CFP on an annual basis, or more regularly if deemed necessary.
- Organize training sessions for staff on various compliance-related issues.
- Remain informed on local and international developments in AML/CFT/CFP and make suggestions to management for improvements.
- Prepare periodic reports on the casino's efforts against money laundering, financing of terrorism, and financing of proliferation.
- Liaise with law enforcement authorities.
- Manage Investigation Order requests received from the authorities.

A Money Laundering Reporting Officer (MLRO) is appointed to be the business owner of AML/CFT/CFP Risk Assessment, Controls, Policies and Procedures. The MLRO appointed should possess professional experience, training and resources to carry out his/her appointment as per Applicable Laws.

5.1. Notification of FIU of unusual transactions conducted by customers

The Company will report unusual transaction or any intended unusual transaction to the FIU without delay. In order to do this, the Company establish clear procedures for internal and external reporting of unusual transactions in place. All unusual individual transactions or series of transactions are to be reported internally, without any delay. Also supporting documents must be submitted as part of the reporting.

The following customers' transactions or intended transactions are deemed unusual:

a) transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;

b) transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);

c) transactions in the amount of XCG. 5,000 (€2500) or more, regardless whether the transaction is made through electronic or other non- physical means. This includes but is not limited to:

i) a cashless transaction in the amount of XCG. 5,000 (€2500) or more. A cashless transaction is a transfer from a bank account of the Company to a local or international bank account, at the request of the client.

ii) accepting or releasing a deposit in the amount of XCG. 5,000 (€2500) or more at the request of the client;

iii) sale to a customer of chips in the amount of XCG. 5,000 (€2500) or more ("chips" include but is not limited to tokens and credits);

For the purpose of performing its obligations, the Company using access to the "goAML" reporting portal after validation by the FIU. The MLRO must prepare a report of all unusual transactions for external reporting to the FIU according to the reporting regulations of the FIU.

5.2. Notification of Fraud, Law Enforcement or Regulatory Authorities' requests

The Company may occasionally receive requests for information or notifications from regulatory authorities or law enforcement bodies in relation to investigations of a criminal, civil or regulatory nature.

When such requests for information are received, these are to be forwarded in their entirety to the MLRO.

Depending on the nature of the request and whether the request for information the Company (through the) will handle and process these requests in line with the following process in which the appointed officers will:

- Record the receipt of such a request;
- Verify the legitimacy of the requesting organisation and individual making this request;
- Verify the legal basis under which such a request is made;
- Inform the requesting organisation that the request is being looked into and provide the appropriate contact information for the legal counsel and MLRO;
- Identify the customer (or customers) accounts relevant to the request;
- Analyse the customer's information, including amongst others due diligence, transactions and ongoing monitoring information;
- Re-consider the customer's risk status considering the received request and take appropriate action depending on the case;
- Identify information that is relevant to the request and following a due assessment of the information, prepare for provision to the requestor, if any; and
- Update the Company records in respect of such a request and where appropriate, notify the relevant regulators or authorities with follow-up actions as per relevant regulatory obligations.

This process needs to be carried out with the assistance and/or guidance of the legal counsel, the MLRO or their delegated appointee. Where appropriate, internal SAR/STR escalation may be considered for review by the MLRO.

The Company will follow the process outlined above to ensure that such notifications or requests are handled without delay. Within its capabilities, the Company will assist relevant authorities effectively.

Notifications from law enforcement and regulatory authorities may also serve as valid basis to assess the effectiveness of the Company's risk mitigation strategies for Responsible Gambling, Fraud, Money Laundering and Terrorist Funding. Where gaps are identified, the Company will take immediate action to address and resolve such gaps.

6. Transactions monitoring

Customer deposits and withdrawal requests are monitored every day to monitor for ML/FT/FP, Fraud and Payments concerns and to enable the business to improve its response to risks involved.

6.1. Deposit monitoring

Document Classification: Company Confidential

Every morning, a search is made in the CMS for new deposits effected in the previous 24 hours by the Management.

The deposit list is extracted from the system and the AML Department analyses any transaction which may be considered as suspicious or which may involve a high risk of fraud. Consideration is also to be taken for customers whose depositing patterns indicate potential responsible gambling concerns.

Deposits are assessed taking into consideration, on a case by case basis, amongst other checks:

- verification, due diligence and risk profile of customer;
- registration, login IP addresses geo-location and distance to customer's address;
- device used to access the customer's account;
- whether the deposit amount and method are reasonable in relation to the customer's risk profile;
- confirm the payment origin matches registration data location;
- confirm to the best practical extent possible that the payment method belongs to the registered customer;
- whether the same payment method has been used on another customer's account;
- history of deposits and amounts, identifying if a customer has reached Customer Due Diligence thresholds;
- Gaming patterns (if necessary, by contacting other internal product teams and/or 3rd party suppliers);
- pending / processed withdrawals;
- past activity and communication with customer;
- any other checks needed depending on the customer's risk assessment.

Suspicious payments in relation to fraud are further investigated and where necessary, customer is contacted to provide explanations or further documentation in respect to identification of customer, payment method and/or source of funds or wealth to ensure affordability.

Temporary suspension of the customer's account or the ability to deposit whilst awaiting feedback from the customer may be considered, in which case the customer is to be informed via e-mail. In such an e-mail, the reasons for the suspension and the information or documentation needed are to be clearly stated.

Customers not having completed the CDD procedure since the moment of completing registration procedure will be sent a template e-mail for completing CDD once they having deposited/withdrawed XCG. 4,000 (€2,000) using any payment methods.

Customers having deposited/withdrawed XCG. 4,000 (€2,000) since the moment of completing registration procedure from a low to medium risk payment method or XCG. 2,000 (€1,000) with a high-risk payment method since the abovementioned moment will be asked to complete the Customer Due Diligence (CDD) procedure (Refer to Annex No. 4 Payment Risk Matrix and to the Customer Due Diligence Procedures).

Customers who have been requested to complete the CDD Procedure may be allowed to continue using their gaming account, but are not allowed to deposit funds into the account effect withdrawals until the procedure is completed.

Customers whose activity will be considered as potential High Risk of potential ML/FT/FP must be reported immediately to the MLRO if suspicion, knowledge or reasonable

grounds to suspect a ML/FT/FP event is present (Refer to Internal Suspicious Transaction Report (STR) Procedure). Where appropriate, these customers will be requested to complete the Enhanced Due Diligence Procedure within thirty (30) days.

The Company pays special attention to clients who:

- Use three or more different payment methods in a short timeframe;
- Frequently switch deposit/withdrawal methods (e.g., more than three times within three months).

In such cases, the client may be reclassified to a Medium or High Risk category, triggering additional verification (EDD) and documentary proof of ownership for each payment method. If the client refuses to supply the requested documentation, the Company may suspend further transactions until the matter is resolved.

After having examined an account into which a deposit has been made, the Customer Risk level needs to be re-assessed and updated. Management must place relevant notes in the customer notes field stating checks done where changes to customer behavior has been noted.

No specific notes must be left in the customer notes section to state that an Internal STR has been raised as this is confidential information that must be known only to the person flagging the concern and the MLRO.

Tipping off a customer that suspicions have been noted or escalated is a criminal offence with potential of serious criminal prosecution that may result in high fines, years of jail-time penalties and a tainted criminal record which would limit the employee from further employment within relevant positions.

6.2. Attempted deposits

A special check is also to be made for customers who tried to make a deposit but failed. For this purpose, in CMS or Payment Gateway Backend, check must be made to filter all customers who in the previous 24 hours attempted (but were not always successful) to deposit funds in their account and sort the list by Customer ID (oldest first) and move through the list to identify:

- customers attempting to deposit multiple times to bypass single amount thresholds;
- customers attempting to deposit using different payment methods;
- customers attempting to deposit different amounts in descending or suspicious patterns;
- customers trying to use deposit whilst under restrictions or when limited;
- customer attempting to use stolen or lost cards (look at failure reason).

6.3. Closed loop policy

The Company operates a stringent closed loop policy on deposits and withdrawals effected by customers.

Where possible, customers must withdraw funds to the originating funding method and cover deposits made before the Company allows withdrawal to a secondary payment method that was used to make deposits, but funds were not used for gaming.

Document Classification: Company Confidential

In each case, customer must prove ownership of that deposit/withdrawal method before any withdrawal is allowed, irrespective of the withdrawal amount.

6.4. Withdrawal monitoring

Every morning, before deposit checks are processed, pending withdrawal requests are to be extracted from the CMS.

AML Department is to check each withdrawal request and assess on a case by case basis:

- verification, due diligence and risk profile of customer;
- whether the customer is precluded from withdrawing due to a pending Due Diligence request;
- registration and login IP addresses geo-location and distance to customer's address;
- device used to access the customer's account;
- whether the withdrawal amount and method are reasonable in relation to the customer's risk profile;
- whether the withdrawal method destination matches registration data location;
- whether withdrawal method belongs to the registered customer;
- whether the same payment method has been used by other customer accounts;
- whether withdrawal method matches a previously used deposit method to enforce closed loop;
- history of deposits and withdrawals;
- Gaming patterns;
- other pending / processed withdrawals;
- device type usage;
- past activity and communication with customer;
- any other checks needed depending on the customer's risk assessment.

Further actions following the above checks may include:

- Freeze the withdrawal when:
 - it is suspected that the customer has broken any provisions of public policies (etc. Terms and Conditions) in order to abuse of promotions and/or exploit any weakness in the Gaming System;
 - customer has not yet provided verification documents for CDD purposes or funding method verification;
 - the payment method to which the withdrawal has been requested is not the same as the funding method (If the funding method does not accept withdrawals, withdrawal has to be sent to a Bank Account registered in the customer's name and verified as such. If deposit was made by a card, the destination payment method of preference in such a circumstance would be the Card's linked Bank Account.).

Where the risk assessment following the above checks indicate a risk of fraud or potential ML/FT/FP, the withdrawal should be marked and put on hold whilst further actions are taken, such as:

- checking customer information with payment providers or verification services provided in case of suspected fraud, or
- placing withdrawal on hold (not visible to customer, no specific note placed into the account stating this) whilst an Internal STR is raised to the MLRO as per the Internal suspicious Transaction Report (STR) Procedure.

If the withdrawal is legitimate and no further actions need to be performed, the withdrawal will be processed unless the amount being withdrawn is equal to, or greater than XCG. 20,000 (€10,000).

Withdrawal requests for XCG. 20,000 (€10,000) or greater, (a similar total of various linked withdrawals is to be considered as triggering this limit), are to be authorised by the Manager responsible for fraud and payments, or, in the case of a sole processing agent, by the immediate senior in a four-eyes principle methodology to mitigate the risks of erroneous payments or internal fraud. The Head of Finance is also to be informed of such withdrawals

An approval for a transaction equal to or over XCG. 20,000 (€10,000) must be given in writing (i.e. e-mail) and recorded for each transaction after it is investigated, and all necessary due diligence, anti-fraud and regulatory requirements have been satisfied. A template e-mail is attached within Annex 9.

7. Employee Training

Within an appropriate period of the commencement of employment, employees are to be provided with ML/FT/FP training to ensure they are aware of measures, policies, controls and procedures that are in force. This training shall include:

- general awareness of Money Laundering / Terrorism Funding for all employees;
- specific Guidance on the related measures, controls, policies and procedures in place within the Company for employees specifically occupying roles related to AML/CFT/CFP Controls and Compliance;
- an assessment to ensure that the employee has grasped the key points of training received.

The training provided to employees is to be recorded and refreshed at least annually. Training includes setting out rules of conduct governing employee's behavior and their ongoing education to create awareness of the Company's Policies against money laundering and terrorist financing. Training process and its contents differs from the type of employees to be trained: new employees, audit staff, AML compliance staff, supervisors and managers, senior management and board of directors and etc. and is conducted in accordance with applicable laws and regulations.

The MLRO is also required to attend annual refresher training and to keep up to date with the subject.

In order to be able to demonstrate that it has complied with the guidelines with respect to training, the Company will maintain records which include:

- details of the content of the training programs provided;
- the names of the person(s) who have received the training;
- the date on which the training was provided;
- the results of any testing carried out to measure the participants' understanding of the AML/CFT/CFP requirements; and
- an ongoing training plan.

Further information about employee training may be found in the Human Resources' relevant policies and procedures.

8. Employee Screening

The Company's prospective employees that are to be involved with or connected to activities that would fall within the scope of this Policies, are to be screened before they are employed. The Company is to ensure that they are fit and proper to occupy positions in which they will participate in the provision of services to the customer. Third party screening providers may be engaged to ensure this.

The Company will carry out monitoring of the activities of its employees during their employment to identify concerns of internal fraud or other criminal activity potentially affecting the Company's operations and obligations. The Company will at all times do its utmost to respect the privacy of its employees.

Employees are also encouraged to report internal suspicious or fraudulent activity by employees to the MLRO and / or Director directly and should they wish to remain anonymous, to do this via an anonymous letter or e-mail service providing as much facts and information as possible.

9. Retention of Records

The Company will maintain, for at least five years, all necessary records on transactions to enable them to comply with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Such records may include:

- all registration details;
- identification verification details;
- standard and enhanced due diligence items;
- suspended accounts and reason for suspension;
- closed accounts;
- financial transactions – deposits, bets made, withdrawals, prize payments;
- self-exclusion periods (temporary and permanent);
- self-imposed limits;
- excluded players;
- complaints and responses;
- audit trails;
- bank reconciliations;
- Customer Service electronic correspondence records.

All records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence must be kept for at least five years after the business relationship is ended, or after the date of the occasional transaction.

End of the customer relationship is defined as from the last day the customer effected any movement of funds to and from their account, or a successful login.

Should statutory obligations arising from other laws, regulations or based on a request from a regulator, a requirement be established to keep records for a longer period be in place, this will be taken in consideration and adhered to.

Documents will not be retained beyond the required obligations and will be deleted.

10. Effectiveness Review

10.1. Initial steps

Document Classification: Company Confidential

The IAF's first action is to carry out identification of the following:

- current legislation in force, noting whether any of this has been changed since the last audit;
- relevant regulators' updated regulations or guidance notes issued since the last audit;
- internal business partners with which the IAF will need to consult during the audit; and
- obtain the latest versions of the Company's Business AML/CFT Risk Assessment, Policies and Procedures applied within the Company.

10.2. Business Risk Assessment review

The IAF will, on a periodical basis in any case not less than once annually, revisit the current Money Laundering, Terrorist Financing and Fraud Business Risk Assessment & consider whether changes have occurred within the business, amongst which:

- 1) Have regulatory requirements changed since the last business risk assessment?
- 2) Has the business changed its targeted customer segments or is it experiencing a change in its main customers' profile type?
- 3) Has the business launched new products?
- 4) Has the business changed any of its Payment Methods?
- 5) Has the business branched into, or stepped out of some geographical markets?
- 6) Has the business launched new ways of interacting with the customer and how to deliver its services?

If the answer to any of these questions is in the affirmative, the Business Risk Assessment areas relevant to that change need to be reviewed and consideration of the effect of such changes in operations should be taken into the context of their implications on the Risk Matrixes. The customer risk assessment should also be considered for review and updating depending on the effects on business risks of the changes.

10.3. AML/CFT Procedures Quality Assurance

i. PEP / Sanction Lists Re-Check

The customer database for customers having registered and been active within the previous 2 years is to be retested.

The Company is required, in relation to exposed PEPs, whether as customer or beneficial owner, to:

- Have appropriate risk-management systems to determine whether a thoroughly risk assessed has been conducted to identify PEP and Sanction countries or individuals;
- Obtain Management approval for accepting any PEP as a customer;
- Take reasonable measures to establish the source of wealth and the source of funds;
- Carried out enhanced ongoing monitoring.

A log of any identified Sanctionable customers and the actions taken on their identification must be produced for review, including any escalations to the relevant reporting authority. Any instances of unflagged PEPs or Sanctionable customers must be thoroughly investigated and the reasons for not having been flagged identified. Remedial steps will be discussed with the relevant personnel and/or suppliers to ensure that such incidents are not repeated.

Note: although stricter Customer Due Diligence is required for each PEP, this Customer Due Diligence does not be the same for every PEP. The measures are tailored to the risk of the PEP, where the following is taken into consideration:

- The type of public function of the PEP;
- The country from which the PEP originates;
- The transactions that the PEP carries out.

Important: the requirements for all types of PEP should also apply to family members or close associates of such PEPs.

ii. Sampling of Customers

A representative sample of customers who have been active since the last AML/CFT and Anti-Fraud effectiveness review must be identified within the players' database or received via a report.

Sampling must take into consideration the higher risk areas identified in the business risk assessment and a larger sample of customers within this group are to be selected for review.

The following controls/measures must be checked on the sample group:

- Initial registration safeguards have been effective (e.g. no accounts with similar e-mail / mobile phone details, no underage or fake looking registrations, no customers having been previously banned by the business or of their own will, or hold a previous account etc.);
- Customers' login access is from registration country;
- Customers' deposits and withdrawals have been monitored and where applicable, questioned;
- Customer's gaming activity has been reasonable and if deviated from normal parameters, that this has been reviewed and noted; and
- Closed loop policy has been adopted for withdrawals, where possible.

Registration Statistics, at a high level, need to be analyzed and compared to previous audits levels to identify changes in registration patterns. These would include assessing the number of registrants per country and % of total registrations and conversions in period and lifetime.

iii. Customer Due Diligence checks

The review is to analyze a representative sample of customers that should have triggered the CDD process based on any of the following conditions, the customer:

- Has been given a high-risk rating in the risk assessment;
- Has made deposits using low-medium risk payment methods totalling XCG. 4,000 (€2,000) or more (all amounts hereinafter are indicated in XCG., approximate EUR equivalents are provided for simplification and rounding purposes only, based on publicly available exchange rate information, in the event of any currency fluctuations, XCG. shall prevail for calculation purposes);
- Has made deposits using high risk payment methods totalling XCG. 1,000 (€500) or more; and
- Has made single or cumulative withdrawals over XCG. 2,000 (€1,000).

In the review, the following areas need to be reviewed:

- Whether customer risk assessment level was efficient to flag a customer for the CDD process and the customer's assessed risk rating was correct;
- The communication process with the customer to ensure that the correct documents were requested as per Risk Based Approach and CDD Procedure;

- The documentation received is stored correctly, sufficient, valid and the correct information was entered in the player management system to record this;
- The customer has been guided accordingly if the documentation was not sufficient; and
- Assess if customers refusing to provide documentation were re-assessed and if needed, SAR/STR raised to the MLRO.

In the case of documentation having been collected through third parties, the same criteria as above must be considered. Receipt of copies of documentation is to be confirmed and tested on a larger sample for documentation collected and provided by agents/intermediaries.

iv. High Depositors / Balance / Winners Checks

A representative sample of customers who have met one or more of the following criteria are to be identified:

- Deposited a lifetime amount of XCG. 40,000 (€20,000) or more;
- Hold a balance of XCG. 40,000 (€20,000) in the customer's account, across all wallets and including any unsettled bets balances; or
- Requested withdrawals amounting to a cumulative total of XCG. 40,000 (€20,000) or more.

The representative sample are to be assessed and ensured that:

- All checks from registration level to onboarding stage have been carried out;
- Customer activity (logins, deposits/withdrawals, payment methods, gaming patterns etc.) has been thoroughly checked and notes have been placed by the relevant employees of the Company;
- Due Diligence Documentation has been obtained;
- Customer risk assessment is in line with customer risk profile; and
- If a customer's activity ought to have triggered an SAR/STR, this has been in fact escalated.

v. Technology Risk Analysis

During the above checks, an analysis has to be made in respect of the controls, that are reliant upon the correct functioning of automated processes, to ensure that these are functioning as expected.

10.4. Internal SAR/STR Reports

SAR/STR Reports' logs are to be retrieved and detailed analysis carried out.

For the analysis to be carried out, identify the number of SAR/STR reports raised since the last review, by processing records kept within the SAR/STR logging system. Statistical information is to be compiled to identify:

- the number of Internal SAR/STR reports;
- customers origin;
- PEP status;
- number and value of transactions;
- categories of suspicious activity;
- completeness of internal SAR/STR report and whether additional information had to be requested from escalating officer;
- external escalation rates;

- time in days to escalate externally;
- underlying reasons for decisions not to escalate SAR/STR externally; and
- customer status following Internal SAR/STR escalation.

A representative sample of customers on whom an SAR/STR has been raised are to be checked for any potential “tipping off” risks via the Company communication systems in breach of AML/CFT rules.

10.5. External Escalations

Escalations carried out to the Relevant Authorities (RA) are to be identified and a representative sample analyzed to identify:

- time taken from initial escalation of the internal STR report to the time when it was escalated externally;
- escalation confirmation received from RA;
- whether any follow up query from RA was received and the time it was taken to respond;
- whether the external escalation resulted in measures having to be taken in respect of customer(s) at the request of the RA;
- whether the customer was allowed to operate normally or under enhanced monitoring with reporting to RA of any customer actions (e.g. attachment order); and
- whether the external escalation triggered a review of internal procedures and/or guidance to analysts.

10.6. Internal ML/FT Risks

i. Employees’ Suitability

In collaboration with the Human Resources Manager, assess:

- HR Policy and Procedures;
- changes in employees complement for employees in positions having a high degree of exposure to AML/CFT risks and the reasons thereof;
- whether relevant documentation has been obtained from new employees;
- whether checks have been done to ensure the validity of the documentation provided;
- whether any of the employees have undergone disciplinary proceedings within the Company and the reasons thereof; and
- whether any internal whistleblowing reports concerned employees in AML/CFT concerned areas.

ii. Employees’ Training

In collaboration with the Human Resources Manager, obtain:

- list of employees that are involved in financial activities of the customers;
- log of AML/CFT awareness training attendees since last review and the results obtained in the assessments undertaken by attendees;
- copy of AML/CFT awareness training materials including assessment questions/answers; and
- records of further AML/CFT training delivered to key personnel, training details reports and certificates.

Carry a review to establish:

- all employees exposed to ML/TF risks have been given basic AML/CFT awareness training and these obtained at minimum a pass mark in the assessment;

- any employees not obtaining a pass mark were offered the opportunity to re-take the training and in the aftermath, obtain a pass mark in the assessment;
- confirm appropriate actions were taken in those cases where an employee failed to obtain a pass mark in the awareness training assessment; and
- AML/CFT awareness training materials are suitable to meet AML/CFT training obligations.

A representative sample of trained employees may be invited to provide their feedback on this training to verify that:

- they have obtained a good level of awareness of ML/TF risks; and
- the training was relevant for them to be aware of ML/TF risks during their daily tasks.

iii. Technology Risk

At this stage, identify which technological measures are applied in the management of ML/TF risks and grade them in accordance with their level of importance (e.g. critical, essential, desirable) to mitigate these risks.

Analyze the function of these technological measures and ensure that:

- the technological measures that are of critical and essential importance function as intended by running tests on a representative sample of events that these should be controlling, for example:
 - verification of e-mail addresses and phone numbers;
 - geolocation data-based checks and automatic redirection or suspension of service and/or PEP and SL checks;
 - risk management software efficacy in flagging unusual activity or suspicious transactions;
 - monitoring tools confirmed to be able to monitor all data in scope for AML/CFT operations;
 - access to sensitive data (such as Customer Risk Assessment Status) being restricted to the appropriate personnel.
- the technological measures are appropriate to mitigate the risk for which they are applied; and
- the technological measures effectiveness' is monitored or reviewed regularly, and fall-back systems are in place should there is a marked degradation or down-time of the service.

10.7. Audit Report

The results and recommendations derived from this AML/CFT audit are to be included in the committee's report to the Audit Committee / Director.

Approved by
Philip M. Humme, o.b.o. Allyant
 Group B.V. as Managing director

Philip M. Humme

Annex No.1 | References

Applicable Laws means the following:

National regulations:

- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G. 2009, no. 65 (N.G. 2010, no. 41) (NORUT) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- The National Ordinance on Identification of Clients when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2009, no. 66 (N.G. 2010, no. 40) (NOIS) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- The National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification of Clients when rendering Services. (National Decree containing general measures on Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70);
- Sanctions national decree Al-Qaida c.s., the Taliban of Afghanistan c.s. Osama bin Laden c.s., and terrorist to be designated locally (N.G. 2010, no. 93);
- National Ordinance on the Obligation to report Cross-border Money Transportation (N.G. 2002, no. 74) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;

These laws and decrees serve as the basis for the procedures maintained by the financial sector of Curaçao to detect and deter industry related risks for money laundering, the financing of terrorism or other criminal activities.

International regulations:

- Caribbean Financial Action Task Force regulations www.cfatf-gafic.org.
- FATF regulations – www.fatf-gafi.org – High-risk and other monitored jurisdictions (published on FATF Website and updated regularly).
- United Nations - Financial Sanctions Consolidated List.
- European Union – Consolidated list of sanctions, AML/CFT/CFP Information page.

Approved by
Philip M. Humme, o.b.o. Allyant
Group B.V. as Managing director

Philip M. Humme

Annex No. 2 | Glossary of Terms

- AML – Anti-Money Laundering
- CDD – Customer Due Diligence
- CFT – Combatting the Financing of Terrorism
- CFP – Combating the Financing of Proliferation of weapons of mass destruction
- EDD – Enhanced Due Diligence
- DE – Designated Employee
- FATF – Financial Action Task Force (www.fatf-gafi.org)
- MLRO – Money Laundering Reporting Officer
- PEP – Politically Exposed Persons
- RBA – Risk Based Approach
- SAR – Suspicious Activity Report
- SDD – Simplified Due Diligence
- STR – Suspicious Transaction Report

Approved by
Philip M. Humme, o.b.o. Allyant
Group B.V. as Managing director

Philip M. Humme

Annex No.3 | Duplicate account criteria

An automatic system carries out a validation check on the registration data looking for any occurrences of similar data in the database which should be unique to an individual. Such occurrences could indicate that the player is trying to open a second account or possibly is unaware that he/she already has an existing account.

Examples:

- similar username or e-mail address;
- similar name, surname, date of birth;
- similar surname and address / postcode;
- similar IP address within previous 24 hours (unless IP matches a whitelist); or
- customer matches at least 2 fields from a blacklist of unwanted customers (fraudsters, self-excluders, abusers etc.).

Attempts at creating multiple accounts could be due to Money Laundering, Fraud, Responsible Gaming Issues etc.

When a registration is accepted, the IP address of the computer from where the registration validation took place is recorded. This can be used during KYC as a source of validation to confirm the country of residence.

Furthermore, the system has a build-in check to refuse registration from IPs which have been previously (within the last few hours) been used to register accounts and were unsuccessful.

Each time a registration is refused, a message is returned to the user as to why the registration was unsuccessful and an e-mail is sent to customer support and technical personnel. This information can be used to track specific individuals who may attempt to create an account at a later stage or may have successfully registered accounts previously.

In those cases where the registration details are suspiciously similar, the registration is processed successfully from the customer's perspective, but a warning e-mail is sent to customer support to investigate further. In most cases, these would be false positives but, on some occasions, it could identify users trying to be clever and bypassing controls on the registration page.

Approved by
Philip M. Humme, o.b.o. Allyant
Group B.V. as Managing director

Philip M. Humme

Annex No.4 | Payment methods risk matrix

The Company's Accepted Payment Methods are listed in bold under the associated categories:

PAYMENT METHODS	Low	Low - Medium	Medium	Medium - High	High	Prohibited
Bank Transfers (EEA or equivalent Safeguards) [e.g. Bank Transfer / Envoy BT]	X					
Debit/credit cards issued by banks [e.g. Visa / Mastercard]	X					
Debit/credit cards issued by other licensed financial institutions [e.g. Visa / Mastercard]	X					
EEA-Licensed payment service providers [e.g. Skrill, Papaya, PayPal, Neteller, EcoPayz, Astropay]		X				
Non-EEA Licensed PSP [e.g. Boleto Bancario, International Bank Transfer, Local Bank Transfer, Astropay]				X		
EEA-Licensed PSP that can be funded with cash or quasi-cash [e.g. Paysafecard E-wallet]				X		
Prepaid cards / vouchers [e.g. Postepay / Paysafecard Vouchers]					X	
Cash [e.g. None available]						X

Approved by
Philip M. Humme, o.b.o. Allyant
 Group B.V. as Managing director

Philip M. Humme

Annex No.5 | Customer type risk matrix

Customer type	Low	Low - Medium	Medium	Medium - High	High
Unverified or front accounts: <i>There is a risk that an account may be opened using false information or by someone other than the registered individual for the purpose of carrying out ML/TF activity. An unverified or front account poses a risk as the Company does not know with whom it is transacting.</i>					X
High-value depositing customers: <i>where a high value deposit is made in a single transaction or cumulative deposits of significant value are made over a short time frame, an increased risk of ML/TF activity is posed – the deposit or deposits may represent the proceeds of crime which the customer intends to launder through, or spend with, the operator</i>			X		
Politically Exposed Persons (PEPs): <i>there is a higher-risk associated with individuals who have a high political profile or have held public office (past or present), as their positions may make them vulnerable to corruption and bribery therefore increasing the risk of accounts being funded by the proceeds of crime by such individuals</i>				X	
Prohibited relationships and transactions (sanctions): <i>there is a risk that an individual subject to sanctions may attempt to open an account and transact with the Company. It is a criminal offence to transact with individuals who are subject to certain types of sanctions such as asset freezes</i>				X	
Dormant: <i>there is a risk that a customer may deposit funds and then not use his account for a significant period of time before looking to withdraw the funds at a later stage, following very little or no activity</i>	X				

Source of funds/wealth is unknown for higher-spending customers: <i>if higher-spending customers are allowed to play without source of funds/wealth being established on a risk-sensitive basis, an increased risk of ML/TF activity is posed</i>				X	
Change to registered personal details for account holders: <i>a customer who changes his personal details such as residential address, email address or telephone number poses an increased ML/TF risk as he may not provide his up-to-date information to an operator. This poses a particular risk where the outdated information is used as part of ongoing monitoring (for example compromising sanctions screening processes) or enhanced due diligence checks and investigations.</i>	X				
Drastic changes in betting behaviour: <i>a drastic change in betting behaviour (i.e. unusually high activity when comparing to what may reasonably be deemed normal expected activity from the customer in question) may indicate that the account is now being used, by the customer or by someone on whose behalf the customer is acting, for money laundering purposes.</i>		X			
Multiple payment methods: <i>individuals using multiple payment methods to fund their accounts without obvious rationale behind such behaviour (e.g. registration of a new credit/debit card to replace an expired one) may be attempting to structure deposits representing the proceeds of crime in order to avoid detection. The use of multiple methods enables an individual to move funds easily to other betting sites or bank accounts. This may include both refundable and non-refundable payment methods</i>		X			
Payment card ownership: <i>where funds are deposited from a card which does not belong to the customer or is a corporate card, there is an increased risk that the customer may be using the card to either deposit unauthorised funds or criminally obtained funds. With corporate cards, there is a risk that a business is being used as a front for criminal activity, therefore corporate cards could be issued</i>	X				

<i>to disguise or transfer the proceeds of crime</i>					
Multiple accounts – same operator: <i>customers are free to spread their activities across a variety of operators, and each operator may therefore have little in terms of transaction history from which to identify unusual behaviour. This may also result in customer activity levels with single operators falling below internal reporting thresholds in accordance with the risk-based approach, where the customer would therefore not be highlighted for further investigation despite significant levels of deposit or drop activity with all operators</i>				X	
VIP enhancements: <i>there is a risk that VIPs are upgraded onto loyalty/reward schemes without having undergone proper due diligence, therefore potentially rewarding customers who have deposited the proceeds of crime with the operator. Additionally, considering the higher monetary values involved in such relationships, should any operator AML/CTF failings be published, they are likely to attract significant national press interest, negatively impacting on public perception of the integrity of the gambling sector</i>			X		
Customer-to customer fund transfers: <i>there is a risk that customers could pass the proceeds of crime from one account to another account held with the same operator (belonging to a different individual) in order to create distance and confuse the money trail or transfer funds as a way of paying for goods or services related to criminal activity.</i>	X				

Annex No.6 | Products/services risk matrix

The Company's Accepted Payment Methods are listed in bold under the associated categories.

Product/Service	Low	Low - Medium	Medium	Medium - High	High
Online Slots	X				
Table Games (including games such as Blackjack, Roulette, Baccarat, and Poker. Live Dealer Games)			X		
Online Poker					X
Progressive Jackpot Games	X				
Virtual Sports Betting		X			
Esports Betting			X		

Approved by
Philip M. Humme, o.b.o. Allyant
 Group B.V. as Managing director

Philip M. Humme

Annex No.7 | Geographical risk matrix

Risk scoring:			
Low	Medium	High	Prohibited
0-19	20-39	40-49	50<
For the sake of simplicity and in accordance to the general practice, the model used in AML/CTF/CDD policy employs progressive scoring- i.e. the higher the score, the higher the risk. Among the "restricted" countries are those that, while having an overall geographic risk score considered acceptable, are nonetheless excluded from engagement by the Company due to applicable legal or licensing requirements and limitations concerning their residents or citizens.			

	Country	Effective score	Risk score
1	Sweden	87	13
2	Norway	87	13
3	Finland	87	13
4	New Zealand	86	14
5	Denmark	85	15
6	Greenland	85	15
7	United Kingdom	85	15
8	Estonia	84	16
9	Slovenia	84	16
10	Lithuania	83	17
11	Malta	82	18
12	Austria	80	20
13	United States	79	21
14	Bhutan	78	22
15	Germany	78	22
16	France	78	22
17	Svalbard and Mayen	77	23
18	Andorra	77	23
19	Saint Pierre and Miquelon	77	23
20	San Marino	77	23
21	Czech Republic	77	23
22	Åland Islands	77	23
23	Guernsey	76	24
24	Belgium	76	24
25	Tokelau	76	24
26	Liechtenstein	76	24
27	Latvia	75	25
28	Jersey	75	25
29	Faroe islands	75	25
30	Ireland	75	25
31	Croatia	75	25

Document Classification: Company Confidential

32	Greece	75	25
33	Poland	75	25
34	Luxembourg	75	25
35	Spain	75	25
36	Isle Of Man	75	25
37	Macedonia	75	25
38	Hungary	74	26
39	Bulgaria	74	26
40	Slovakia	73	27
41	Italy	72	28
42	Romania	72	28
43	Switzerland	72	28
44	Netherlands	72	28
45	Georgia	72	28
46	Portugal	70	30
47	Gibraltar	69	31
48	Cyprus	69	31
49	French Guiana	68	32
50	French Polynesia	68	32
51	Australia	67	33
52	Vatican City State (Holy See)	67	33
53	Canada	66	34
54	Singapore	66	34
55	Kazakhstan	65	35
56	Thailand	65	35
57	Tajikistan	65	35
58	British Virgin Islands	64	36
59	Uzbekistan	64	36
60	Micronesia	63	37
61	Burkina Faso	63	37
62	Saint Martin (French part)	63	37
63	Curacao	62	38
64	Mongolia	61	39
65	South Korea	61	39
66	Hong Kong	61	39
67	Dominican Republic	60	40
68	Congo (Brazzaville)	60	40
69	Vietnam	60	40
70	Philippines	60	40
71	Grenada	60	40
72	Turkey	60	40
73	Bahrain	60	40
74	Macau	60	40
75	Iceland	60	40
76	Cook Islands	60	40
77	British Indian Ocean Territory	60	40
78	Pitcairn	60	40
79	Saint Helena, Ascension and Trista	60	40

Document Classification: Company Confidential

80	Belize	59	41
81	Cuba	59	41
82	Belarus	59	41
83	American Samoa	59	41
84	Maldives	59	41
85	China	59	41
86	Armenia	58	42
87	South Africa	58	42
88	Guyana	58	42
89	Madagascar	58	42
90	Albania	58	42
91	Guadeloupe	58	42
92	Martinique	58	42
93	Mayotte	58	42
94	New Caledonia	58	42
95	Réunion	58	42
96	Saint Berthélemy	58	42
97	Zambia	58	42
98	Bermuda	58	42
99	Montserrat	58	42
100	United Arab Emirates	58	42
101	Namibia	58	42
102	Anguilla	57	43
103	Sri Lanka	57	43
104	Brunei Darussalam	57	43
105	Ukraine	57	43
106	Christmas Island	57	43
107	Cocos (Keeling) Islands	57	43
108	Norfolk Island	57	43
109	Japan	57	43
110	Malawi	57	43
111	Azerbaijan	57	43
112	Malaysia	57	44
113	Aruba	56	44
114	Ethiopia	56	44
115	Tonga	56	44
116	Chile	56	44
117	Montenegro	56	44
118	Oman	56	44
119	India	56	44
120	Brazil	56	44
121	United States Virgin Islands	56	44
122	Fiji	56	44
123	Serbia	56	44
124	Marshall Islands	56	44
125	Jamaica	56	44
126	Dominica	56	45
127	Algeria	55	45

Document Classification: Company Confidential

128	Cayman Islands	55	45
129	Vanuatu	55	45
130	St Vincent & Gren	55	45
131	El Salvador	55	45
132	Lesotho	55	45
133	Honduras	55	45
134	Falkland Islands (Malvinas)	55	45
135	Taiwan	55	45
136	Eritrea	55	45
137	Qatar	55	45
138	Bangladesh	55	46
139	St Maarten	54	46
140	Costa Rica	54	46
141	Tunisia	54	46
142	Equatorial Guinea	54	46
143	Mauritius	54	46
144	Kyrgyzstan	54	46
145	Nauru	54	46
146	Puerto Rico	54	46
147	St Kitts & Nevis	54	46
148	Timor-Leste	54	46
149	Russian Federation	54	46
150	Argentina	54	46
151	Indonesia	54	46
152	Barbados	54	46
153	Israel	54	46
154	Gambia	54	46
155	Uganda	54	46
156	Benin	54	46
157	Palau	54	46
158	St Lucia	54	46
159	Moldova	54	46
160	Antigua and Barbuda	54	46
161	Mexico	54	46
162	Tuvalu	54	46
163	Uruguay	54	47
164	Botswana	53	47
165	Niger	53	47
166	Suriname	53	47
167	Cape Verde	53	47
168	Turks & Caicos	53	47
169	Togo	53	47
170	Colombia	53	47
171	Niue	53	47
172	Wallis and Futuna	53	47
173	Egypt	53	47
174	Bosnia-Herzegovina	53	47
175	Kosovo	53	47

Document Classification: Company Confidential

176	Turkmenistan	53	47
177	Nepal	52	48
178	Rwanda	52	48
179	Kuwait	52	48
180	Cameroon	52	48
181	Solomon Islands	52	48
182	Bonaire, Sint Eustatius and Saba	52	48
183	Seychelles	52	48
184	Peru	52	48
185	Mauritania	52	48
186	Senegal	52	48
187	Papua New Guinea	52	49
188	Monaco	51	49
189	Sao Tome & Prin.	51	49
190	Samoa	51	49
191	Sierra Leone	51	49
192	Comoros	51	49
193	Angola	50	50
194	Trinidad & Tobago	50	50
195	Bahamas	49	51
196	North Mariana Islands	49	51
197	Congo, the Democratic Republic	49	51
198	Cambodia	49	51
199	Panama	48	52
200	Haiti	48	52
201	Saudi Arabia	48	52
202	Kiribati	48	52
203	Guam	48	52
204	Cote D'Ivoire	47	53
205	Djibouti	47	53
206	Paraguay	47	53
207	Guinea	47	53
208	Gabon	47	53
209	Venezuela	46	54
210	Chad	46	54
211	Swaziland (Eswatini)	46	54
212	Jordan	46	54
213	Libya	45	55
214	South Sudan	45	55
215	Zimbabwe	44	56
216	Guinea Bissau	44	56
217	Pakistan	43	57
218	Iraq	43	57
219	Tanzania	43	57
220	Nicaragua	42	58
221	Lebanon	42	58
222	Mozambique	41	59
223	Kenya	41	59

224	Guatemala	41	59
225	Ghana	41	60
226	Myanmar	40	60
227	Morocco	40	60
228	Western Sahara	40	60
229	Bolivia	39	61
230	Lao People's Democratic Republic	39	61
231	Ecuador	38	62
232	Somalia	38	62
233	West Bank (Palestinian Territory)	37	63
234	Mali	37	63
235	Liberia	37	63
236	Gaza Strip	37	63
237	Central African Republic	36	64
238	Nigeria	36	64
239	Syria	35	65
240	Burundi	34	66
241	Sudan	33	67
242	Yemen	33	67
243	Afghanistan	32	68
244	North Korea	21	79
245	Iran Islamic Republic	18	82

Approved by
Philip M. Humme, o.b.o. Allyant
Group B.V. as Managing director

Philip M. Humme

Annex No.8 | Client Risk Level Matrix

RISK TYPE				Final Risk Level
Geographical	Customer Type	Products/Services	Distribution Channels	
Low	Low	Low	Low	Low
Low	Low	Low	Medium	Low
Low	Low	Low	High	Low
Low	Low	Medium	Low	Low
Low	Low	Medium	Medium	Low
Low	Low	Medium	High	Low
Low	Low	High	Low	Low
Low	Low	High	Medium	Medium
Low	Low	High	High	Medium
Low	Medium	Low	Low	Low
Low	Medium	Low	Medium	Medium
Low	Medium	Low	High	Medium
Low	Medium	Medium	Low	Medium
Low	Medium	Medium	Medium	Medium
Low	Medium	Medium	High	Medium
Low	Medium	High	Low	Medium
Low	Medium	High	Medium	Medium
Low	Medium	High	High	High
Low	High	Low	Low	Low
Low	High	Low	Medium	Medium
Low	High	Low	High	Medium
Low	High	Medium	Low	Medium
Low	High	Medium	Medium	High
Low	High	Medium	High	High
Low	High	High	Low	Medium
Low	High	High	Medium	High
Low	High	High	High	High
Medium	Low	Low	Low	Low
Medium	Low	Low	Medium	Medium
Medium	Low	Low	High	Medium
Medium	Low	Medium	Low	Low
Medium	Low	Medium	Medium	Medium
Medium	Low	Medium	High	Medium
Medium	Low	High	Low	Medium
Medium	Low	High	Medium	Medium
Medium	Low	High	High	High
Medium	Medium	Low	Low	Medium
Medium	Medium	Low	Medium	Medium
Medium	Medium	Low	High	Medium
Medium	Medium	Medium	Low	Medium
Medium	Medium	Medium	Medium	Medium
Medium	Medium	Medium	High	Medium

Medium	Medium	High	Low	Medium
Medium	Medium	High	Medium	Medium
Medium	Medium	High	High	Medium
Medium	High	Low	Low	Medium
Medium	High	Low	Medium	Medium
Medium	High	Low	High	High
Medium	High	Medium	Low	Medium
Medium	High	Medium	Medium	Medium
Medium	High	Medium	High	Medium
Medium	High	High	Low	High
Medium	High	High	Medium	High
Medium	High	High	High	High
High	Low	Low	Low	High
High	Low	Low	Medium	High
High	Low	Low	High	High
High	Low	Medium	Low	High
High	Low	Medium	Medium	High
High	Low	Medium	High	High
High	Low	High	Low	High
High	Low	High	Medium	High
High	Low	High	High	High
High	Medium	Low	Low	High
High	Medium	Low	Medium	High
High	Medium	Low	High	High
High	Medium	Medium	Low	High
High	Medium	Medium	Medium	High
High	Medium	Medium	High	High
High	Medium	High	Low	High
High	Medium	High	Medium	High
High	Medium	High	High	High
High	High	Low	Low	High
High	High	Low	Medium	High
High	High	Low	High	High
High	High	Medium	Low	High
High	High	Medium	Medium	High
High	High	Medium	High	High
High	High	High	Low	High
High	High	High	Medium	High
High	High	High	High	High

Approved by
Philip M. Humme, o.b.o. Allyant
Group B.V. as Managing director

Philip M. Humme

Annex No.9 | Over XCG. 20,000 (€10,000) Authorisation Template

From: [Agent]

To: [Supervisor / Manager]

Head of Finance / Finance Team

Subject: Over XCG. 20,000 (€10,000) Withdrawal Authorisation – [Amount] – [User ID]

Hi,

User ID [13123124] is requesting a withdrawal of XCG. 26,000 (€13,000) via [Neteller].

Kindly find below the user and transaction information.

User ID:	<i>e.g. 13123124</i>
Customer Category:	<i>e.g. [VIP Level1 / Basic Customer / Long Term etc.]</i>
Registered Date:	<i>e.g. 01/02/2017</i>
Activity Pattern:	<i>e.g. Regular high roller, Occasional Large Gamer, Small gamer</i>
Platforms:	<i>e.g. Sportsbook / Casino</i>
Usual Deposit Methods	<i>e.g. Mostly Card 1234 but Neteller used in last 3 months</i>
Origin of funds being withdrawn	<i>e.g. Built up deposits/winnings, Jackpot etc.</i>
Usual Withdrawal Method	<i>e.g. Card, Neteller</i>
This withdrawal requested to	<i>e.g. Neteller</i>
Adheres to Closed Loop Policy	<i>e.g. Yes</i>
Past Deposit/Withdrawal History of Customer	<i>e.g. XCG. 70,000 (€35,000) Deposited, XCG. 4,000 (€2000) Withdrawn - No previous large jackpots prior to this instance.</i>
Full Anti-Fraud / AML / CDD Procedures passed:	<i>e.g. Yes</i>
Authorisation Recommended?	<i>e.g. Yes / No</i>
Reason if No:	

Approved by
Philip M. Humme, o.b.o. Allyant
Group B.V. as Managing director

Philip M. Humme

Annex No. 10 | Suspicious Activity Report

Report prepared by:	
Business partners	
Name	
Account ID	
Address	
Email address	
Telephone number	
Is identification and address verification held?	
Is enhanced due diligence held?	

Reason for suspicion	
To include: Identification verification Criminal conduct known or suspected	
Date of report	

Receipt of report acknowledged	
Signed by:	Lydia Obispo
MLRO	
Date	May 28, 2025

Approved by
Philip M. Humme, o.b.o. Allyant
 Group B.V. as Managing director
May 28, 2025

Title	AML Policy Galaktika
File name	Galaktika_Anti-Mo...alaktika_N.V.docx
Document ID	a77abf2465334d2733bbb1c73550df5845d2f582
Audit trail date format	MM / DD / YYYY
Status	● Signed

Document History



05 / 28 / 2025
21:50:12 UTC

Sent for signature to Lydia Obispo (lydia.obispo@allyant-group.com) and Philip Humme (philip.humme@allyant-group.com) from gala.serre@allyant-group.com
IP: 190.13.122.21



05 / 28 / 2025
22:40:40 UTC

Viewed by Philip Humme (philip.humme@allyant-group.com)
IP: 206.0.71.10



05 / 28 / 2025
22:41:06 UTC

Signed by Philip Humme (philip.humme@allyant-group.com)
IP: 206.0.71.10



05 / 28 / 2025
23:52:25 UTC

Viewed by Lydia Obispo (lydia.obispo@allyant-group.com)
IP: 190.88.75.74



05 / 28 / 2025
23:53:30 UTC

Signed by Lydia Obispo (lydia.obispo@allyant-group.com)
IP: 190.88.75.74



COMPLETED

05 / 28 / 2025
23:53:30 UTC

The document has been completed.