

Carletta N.V. – Anti-Money Laundering Compliance Policy

6.6.1. The customer risk profile contains the following fields

Username as stored in the back office

When creating an account with the Company the Player selects a username that will be stored within the Company's back office and is used to further identify the Customer. The username itself cannot be utilized to identify the Customer unless access is provided to the secured Company back office and thus anonymization is achieved to satisfy personal data privacy standards/requirements.

Access to personal and risk-related data is restricted and managed in accordance with the Company's internal data protection and security policies. Any linkage between a Player's risk profile and their personal identifiable information is subject to appropriate access controls, ensuring compliance with applicable data protection laws.

Funding method as described in the back office

The Company's back office stores all possible funding methods for all jurisdictions within its back office and allocates these funding methods to Players using them accordingly.

Each funding method contributes to the Player's overall Customer Risk Assessment (CRA) score, in line with the Company's Risk-Based Approach (RBA) and the findings of the Business Risk Assessment (BRA). Players using high-risk payment methods may be subject to Enhanced Due Diligence (EDD) or rejected under the Customer Acceptance Policy (CAP) if their total risk score exceeds the permitted threshold.

Each payment method has received an internal relevant risk score based on the strength of the controls applied to the Customers using said particular payment methods, as well as on the strength of the AML policies and procedures employed by the payment method providers themselves.

The risk scores are described as follows:

Risk Rating	Risk Score	Description
Low	1	• European or EU equivalent bank transfers • Debit cards issued by credit institutions within the EU/EEA or at EU standards
Medium	2	• EU/EEA Credit Card • EU/EEA PSP which does not allow Customers to fund with cash or quasi-cash

Risk Rating	Risk Score	Description
High	3	• Prepaid Cards • Vouchers • NON-EU/EEA Debit card • NON-EU/EEA Credit card • VFAS (cryptocurrencies) • EU/EEA licensed payment providers that can be funded with cash or quasi-cash • Non-EEA licensed PSPs that allow Customers to fund with cash or quasi-cash • NON-EU/EEA which do not allow Customers to fund with cash or quasi-cash.

NOTE: Some of the risk categories found in the above ratings might not be currently present within the Company's risk appetite, however, they have been noted in the general risk assessment as to be used at any future date in case the Company deems it necessary.

The current payment methods have been adjusted to reflect the status of the Company's risk appetite in the individual scores.

Player Jurisdiction

The Company takes into consideration Player jurisdiction upon onboarding to ensure that the country the Player comes from is within the Company's risk appetite.

All countries accepted by the platform have been analyzed based on the individual controls applied by the Company on a case-by-case basis, as well as concatenating information from various online resources that offer insight into the risk specific jurisdictions pose from an AML/CFT perspective.

Each country supported by the platform has been given a risk score based on the data processed from the various resources.

Please refer to **Annex C - Jurisdiction Risk Classification and Prohibited Countries List** for the main documentation used for determining a country's risk rating.

The jurisdiction risk scores are described as follows:

Carletta N.V. – Anti-Money Laundering Compliance Policy

Risk Rating	Risk Score	Description
Low	1	Countries that offer a strong AML/CFT regulation in line with international standards. Countries that offer good AML/CFT regulation and show signs of constant improvement
Medium	2	Countries that offer an acceptable AML/CFT regulation have shown plans to improve in the future. Countries that offer a baseline AML/CFT regulation and controls can be put in place to mitigate risks
High	3	Countries lacking sufficient and/or effective AML/CFT regulation and controls in place to mitigate risks
Blocked/Extreme	N/A	Countries banned via platform to avoid risks from an AML/CFT perspective and countries listed as High-Risk Jurisdictions subject to a Call for Action by the FATF

Player registration channel

The Company offers the possibility of online registration for its Players. Upon registration, Players must provide core identifying details such as full name and date of birth, in accordance with the Company's onboarding and identification procedures. Once the Player deposits and starts to wager, the account is monitored for any increase in risk or high-volume wagering/high amount wagering. Should it be deemed necessary, the Customer will be asked to verify the source of funds even though the relevant thresholds have not been met. Should it transpire that the information and documentation provided at this stage is fake, inaccurate, or incorrect, the account will be suspended, and an investigation will be initiated to determine whether there are sufficient grounds to file an UTR.

Player first deposit amount

The Company considers that the initial sum deposited by a specific Player is crucial in determining the type of behavior the Company needs to exhibit toward the Player from both an AML perspective as well as a Responsible Gambling perspective.

To this extent, the possible first deposit amounts have been broken down into 3 categories beginning with the most common deposit amount and incrementing to the threshold for due diligence requirement.

The deposit amounts are broken down as follows:

Carletta N.V. – Anti-Money Laundering Compliance Policy

Risk Rating	Risk Score	Amounts (XCG)
Low	1	0 to 2,000
Medium	2	2,001 to 4,000
High	3	4,000 +

Player first withdrawal amount

The Company monitors the initial withdrawal amount to determine the type of business relationship the Customer seeks to form with the Company as well as to place monitoring flags on the Customer account for future withdrawal actions and search for any suspicious patterns.

The withdrawal amounts are broken down as follows:

Risk Rating	Risk Score	Amounts (XCG)
Low	1	0 to 2,000
Medium	2	2,001 to 4,000
High	3	4,000 +

6.6.2. Format of Records

The Company's Management shall retain the documents/data mentioned in this Policy, other than the original documents or their certified true copies that are kept in a hard copy form, in other forms, such as electronic form, provided that the Company's Management shall be able to retrieve the relevant documents/data without undue delay and present them at any time, to the FIU or any other relevant authority, after a relevant request.

In case the Company establishes a documents/data retention policy, the Compliance Officer shall ensure that the said policy shall take into consideration the requirements of the Law and the Directives.

The Internal Auditor shall review the adherence of the Company to the above, at least annually.

6.6.3. Certification and language of documents

The documents/data obtained shall be in their original form or as a copy of the original. In high-risk cases or if deemed appropriate, the Company may request documents to be certified as true copies of the original and/or be apostilled. In the case that the documents/data are certified as true

Carletta N.V. – Anti-Money Laundering Compliance Policy

copies by a different person than the Company itself or by the third party with whom a reliance and or intermediary agreement has been reached, the documents/data must be apostilled or notarized or certified by a professional whose identity and professional capacity must be confirmed and verified. In certain high-risk cases, identification and verification of the certifier may also be necessary.

A true translation shall be attached in the case that the documents mentioned above are in a language other than English, or a language which is not known by the person reviewing the document.

6.6.4. Procedures

The procedures and frequency relating to the monitoring of Customers' profiles, accounts, and examination of transactions based on the Customer's level of risk shall include the following:

- (a) the identification of:
 - transactions which, as of their nature, may be associated with money laundering or terrorist financing.
 - unusual or suspicious transactions that are inconsistent with the economic profile of the Customer for further investigation.
 - in case of any unusual or suspicious transactions, the administrator handling the specific Customer as well as the Head of that Department shall be responsible for communicating with the Compliance Officer.
- (b) Further to point (a) above, the investigation of unusual or suspicious transactions by the Compliance Officer. The results of the investigations are recorded separately and kept in the file of the Customers concerned.
- (c) the ascertainment of the source and/or origin of the funds credited to accounts.
- (d) the use of appropriate IT systems.
- (e) For the Company to comply with its monitoring requirements it shall review the Customer's file according to the timeframes, as per section 5.15.3 below, and take into consideration the following to assess whether any additional or replacement documentation/evidence might be required:
 - Update any expired identification documentation
 - Update any changes in the companies' structure and involved people.
 - Changes in the Customers' activities which might have an impact on the Customers' economic profile.
 - Reviewing ways in which new products and services may be used by criminals for money laundering and/or terrorist financing purposes, and how these ways may change to conceal such illicit activities.

- The compliance officer performs checks to ensure that the relevant reviews take place and documentation is kept accordingly.
- Reporting and accountability by the compliance officer to the Board of Directors and Senior Management.
- Liaising with the Curacao Gaming Control Board, FIU, or any other relevant/applicable authority in a case where such liaising is required.

6.6.5. Timeframes

The time frames set below shall act as guidelines for the Compliance Officer when setting the dates for the re-review dates. Such time frames may be changed if justified notwithstanding the Customer has been risked as in a category, provided such justification is recorded. Furthermore, these time frames should be changed and updated should any of the factors affecting the risk the Customer poses change. The below time frames shall be taken as guidance points and not as a mandatory rule.

Risk Classification	Time Frames
Low Risk	12 - 24 months
Medium Risk	6– 12 months
High Risk	3 – 6 months

6.6.6. Payout Management Procedure

Checks to be performed on each pay-out:

a. Account check

The owner of the Carletta N.V. account must be the same person as the owner of the bank account or credit card. All account information, like address, email, date of birth, etc., must be complete and authentic. Withdrawals will be made to the same source where the funds originated (where possible).

b. Deposits must have been used

On each payout, the Company will verify whether the deposits have been used for stakes. All deposit amounts need to have been wagered at least once (1) when a bonus was not credited before a withdrawal request can be made. In the case where a bonus has been utilized, the total amount of deposit and bonus must be wagered at least seven (7) times before being allowed to make a withdrawal. A pay-out cannot be processed if the deposited amount has not been used for stakes.

Carletta N.V. – Anti-Money Laundering Compliance Policy

With reference to the second sentence in this paragraph, if the deposited amount has not been used, the payout has to be denied. Furthermore, the latest winnings have to be checked for correctness.

c. Fulfilment of bonus rules

Before a payout can be deducted from the Customer's account, the account has to be checked if a bonus has been given to the Customer since the last payout. When a bonus has been credited, the account has to be checked for the fulfilment of the bonus rules applicable to that bonus.

If bonus rules have not been fulfilled the requested pay-out cannot be completed.

d. Deposit of funds

Funds deposited in the gaming wallet can only be used for gaming activity. Should Carletta N.V. notice regular changes by Players to the payment method linked to the gaming wallet, the account will be suspended until the necessary explanations are provided by the Player for these changes.

Carletta N.V. does not allow Players to transfer funds between accounts under any circumstances.

The Company's KYC team continuously monitors Players' deposit activity as well and has automated processes in place to receive notifications when Players achieve the XCG 4,000 (four thousand) transaction limit.

e. Risk Profile for Carletta N.V.

The risk profile and risk appetite for Carletta N.V. will be calculated based on the Business Risk Assessment done at a minimum once every year. The Business Risk Assessment will take into consideration all risks the Company faces constantly as well as the mitigating factors controlling the inherent risk. Modifications will be done to the policies and procedures for Carletta N.V. based on the resulting risk, as soon as the need arises.

Withdrawals can only be paid to the same Customer's account used to deposit money. This is in line with p. III.8. of Regulations, which provides that there is a higher transaction risk if the user's card is issued in the name of third parties. Therefore, the funds to be paid to the Player can only be withdrawn to the same account from which the funds paid into the Player's account originated. If the payment method used does not allow Carletta N.V. to settle payouts to the same payment method, then Carletta N.V. must identify and verify that the method used to settle the withdrawal request belongs to the Player in question.

Carletta N.V. does not accept cash from Customers, and funds may only be received through

online transfer. In the same manner, no withdrawals can be processed as cash. Withdrawals will always be remitted to the same account from where the funds originated or to an account or payment method that has been verified as belonging to the Player.

At all times Management shall ensure that the total of all the Players' account funds including any funds in transit shall be at least equal to the aggregate of the amount standing to the credit of the Players' accounts held by the Company to have sufficient funds to pay out the prize money with appropriate ring-fencing and segregation measures as prescribed by per p.5, Art.6 of the Conditions to Curaçao Online Gaming License.

CDD documentation is always requested and verified for all Players affecting a single or cumulative (e.g. in one day) transaction of XCG 4,000 or more or upon requesting to withdraw funds.

The system will automatically stop minors from registering as Players inputting a date of birth below the age of 18 years of age.

6.6.7. Dormant Accounts

If a Player does not log in to his/her Player Account for 180 consecutive days, it will be classified as an "inactive account." The Company will notify the Player via email at least 30 days before the account becomes inactive. Once an account is deemed inactive, the remaining balance will be debited from the account. Following the account becoming inactive, the Company will suspend the account at that time for security reasons. This means that following the Player's request and following completion of any identity verification checks, the Company will restore access to the account. Funds that were debited due to the account suspension are not subject to a refund.

6.7. Reliance on Third Parties to perform Customer Due Diligence

Carletta N.V. relies on the services of **KYCAID LIMITED**, a qualified third-party KYC provider, to conduct specific onboarding and customer due diligence (CDD) activities. These include identity verification, document validation, biometric checks, and sanctions/PEP screening.

Further information regarding the responsibilities of third-party providers and the first line of defense can be found in Section **6.2.8. "First Line of Defense (KYC and Onboarding Staff)"** and Annex A **"Internal Control Structure: Three Lines of Defense"**.

6.8. Unusual Transaction Reporting

Carletta N.V. – Anti-Money Laundering Compliance Policy

In any case, where the Company encounters, verifies or there exists a reasonable suspicion that any form of money laundering is taking place or being attempted, such activity or transaction will be reported to the Financial Intelligence Unit (FIU), as required. The activity or transaction will be reported through the portal for filing and submitting Unusual Transaction Reports (UTR), as designated by the FIU. The Company, through its Compliance Officer, is responsible for ensuring that when an UTR is filed, all supporting documentation and information about why the transactions, as well as the Player, have been flagged as unusual must also be submitted. Any employee and/or Company officer having observed unusual activity from a Customer potentially using the products and/or services of the Company for ML/FT/FP must report such suspicion to the Compliance Officer by not later than 24 hours from when such suspicion is formed. The Compliance Officer, upon receipt of such report, must initiate an investigation into the unusual activity and/or transaction and verify if such suspicion is objectively justified. This is to be done in the shortest time possible. This notwithstanding, the Compliance Officer may continue to investigate to gather the evidence required to submit a complete UTR.

The FATF website is checked regularly to keep abreast with the latest updates and blacklist jurisdictions as well as jurisdictions that do not abide by FATF and other relevant anti-money laundering regulations.

The definition of an unusual transaction and the range of transactions that may be related to money laundering, terrorist financing, or proliferation financing (ML/TF/FP/PF) is broad and not exhaustively defined. Curaçao AML legislation distinguishes between objective and subjective indicators for identifying unusual transactions under the National Ordinance on the Reporting of Unusual Transactions (NORUT) and its implementing National Decree (AB 2017 no. 104). The specific indicators are further established in the Ministerial Decree Indicators Unusual Transactions (N.G. 2015 no. 73).

In accordance with the Ministerial Decree Indicators Unusual Transactions (N.G. 2015 no. 73), the following **objective indicators** apply to casinos, internet gambling operators, and lottery providers, and must be treated as unusual transactions requiring reporting to FIU Curaçao:

- 1) An unusual transaction exists where a transaction has been reported to the police or justice authorities in connection with suspected money laundering or terrorist financing. A proposed transaction is also classified as unusual where it is carried out by, or on behalf of, a natural person, legal entity, group, or organization appearing on a sanctions list established pursuant to the Kingdom Sanctions Act.
- 2) Furthermore, any transaction in the amount of NAf 5,000 or more, irrespective of whether it is conducted in cash, by cheque, by other payment instrument, or via electronic or other non-physical means, constitutes an objective indicator. This includes non-cash transactions of NAf 5,000 or more where funds are transferred from the service provider's bank account

to a domestic or international account at the customer's request; the provision or receipt of monetary equivalents of NAf 5,000 or more; the sale of gaming chips, tokens, or gaming credits amounting to NAf 5,000 or more; and the payout of prize money of NAf 5,000 or more.

In addition to the objective indicators listed above, the Ministerial Decree establishes a **subjective indicator** for gaming operators: a transaction must be treated as unusual where, based on its nature, scope, pattern, or surrounding circumstances, there are reasonable grounds to believe that it may be related to money laundering or terrorist financing, even if no objective threshold has been met.

So, objective indicators are defined by Ministerial Decree and must be reported when triggered, regardless of any suspicion **while subjective indicators** are based on the professional judgment of the Company and its employees.

Unusual activity is typically characterized by transactions or behaviors that are inconsistent with the Customer's known transaction patterns, declared economic profile, or expected deposit and wagering behavior. To reasonably determine whether activity is unusual, multiple contextual elements must be considered in combination.

The Company must ensure that it maintains adequate Customer knowledge and monitoring procedures to detect such anomalies in a timely manner and report them as required. Recognizing a transaction or activity as unusual is essential to triggering internal escalation and potential reporting to the FIU.

Any unusual behavior needs to be reported to the FIU. If FIU Curaçao, after proper analysis of an unusual transaction, concludes that there is a suspicion of ML/FT/FP, this transaction or series of transactions will be reported to the Public Prosecutor's Office.

Examples of what might constitute unusual transactions/activities related to ML/FT/FP are listed in Annex B of this Policy. The relevant list is not exhaustive, nor does it include all types of transactions or services that may be requested to be used, nevertheless, it can assist the Company and its employees (especially the Compliance Officer and the Company's Management) in recognizing the main methods used for ML/FT/FP. The detection by the Company of any of the transactions contained in the said list prompts further investigation and constitutes a valid cause for seeking additional information and/or explanations as to the source and origin of the funds for the payments and intended transactions, the nature and economic/business purpose of the underlying transactions requested, and the circumstances surrounding the activities.

Carletta N.V. – Anti-Money Laundering Compliance Policy

6.8.1. Internal reporting and escalation procedure

Where a frontline employee (First Line of Defense), including Customer Support, KYC, or Fraud personnel, identifies a transaction, pattern, or activity that appears unusual or potentially suspicious, they must submit an Internal Suspicion Report (ISR) to the Compliance Officer within 24 hours of forming such suspicion.

Upon receipt of the ISR, the Compliance Officer shall initiate an internal investigation without delay. This investigation may include, but is not limited to:

- Reviewing the Player's transactional history and behavioral patterns;
- Cross-checking the Customer's profile, documents, and prior risk assessments;
- Analyzing login data and payment instruments used;
- Requesting additional information or documentation from the Customer, such as clarification of the source of funds or source of wealth or supporting documents;
- Contacting the Customer's bank or financial institution, if necessary, to request a reference letter or further validation of account ownership or legitimacy of funds.

If the Compliance Officer determines that the transaction or activity is to be classified as unusual or suspicious under the National Ordinance on the Reporting of Unusual Transactions (NORUT), an Unusual Transaction Report (UTR) shall be submitted without undue delay to the FIU via the goAML platform.

The ISR serves as both the initial notification form and the evaluation document. It is submitted by the First Line of Defense and reviewed by the Compliance Officer, who uses the same report to record investigative steps, internal findings, and the final decision regarding submission to the FIU. This single-report structure ensures accountability, traceability, and operational efficiency. **A standardized template of the ISR is provided in Annex D of this Policy.**

All supporting documentation, internal findings, correspondence, and records of the investigation must be attached to the UTR as part of the submission package.

The Compliance Officer shall ensure that the account in question is flagged for enhanced monitoring or temporarily restricted, if necessary, to prevent further risk while maintaining compliance with anti-tipping-off provisions.

6.8.2. Knowledge

Professional judgment, as a driver to qualitatively assess subjective indicators, is used to ascertain whether there is ML/FT. If for any reason the Compliance Officer, or any other employee of the

Company, is aware or owns information that indicates that any of the above activities may have taken place, are taking place, or will be taking place, the Compliance Officer should immediately proceed with filing a report with the FIU.

To identify unusual transactions, the Compliance Officer shall perform the following activities:

- Monitor continuously any changes in the Customer's financial status, business activities, type of transactions, etc.
- Provide adequate training to all staff who will be in contact with any Customer, agents, Customer's transactional information and/or documentation, operational information and/or documentation, and any other information and/or documentation which can lead to knowledge or suspicion being detected.

6.8.3. Compliance Officer's report to the FIU

All Unusual Transaction Reports (UTRs) are submitted through the goAML reporting portal. After the submission of a UTR, the Company may subsequently wish to terminate its relationship with the Customer concerned for de-risking reasons or to keep the account suspended until further notice/information is obtained from the FIU. In such an event, the Company exercises caution, according to the Law, not to alert the Customer concerned that a unusual transaction report has been submitted to the FIU. Close liaison with the FIU is, therefore, maintained by the Compliance Officer to avoid any frustration to the investigations being conducted. If no information and/or directions are given by the FIU, it shall be up to the Company to decide on the best course of action, whilst at all times ensuring that no tipping-off takes place.

Furthermore, after the submission of an UTR, the Customer's account and services rendered concerned are placed under the close monitoring of the Compliance Officer and cease to be operative if deemed appropriate to do so without tipping-off or risking tipping-off the reported individual or entity.

6.8.4. Submission of information to the FIU

The Company ensures that in the case of an unusual transaction investigation by the FIU, the Compliance Officer will be able to provide without delay the following information:

- a. the identity of the holders for which the services have been provided.
- b. the identity of the Beneficial Owners.
- c. the identity of the persons authorized to act on behalf of the Beneficial Owners.
- d. data of the volume of funds or level of transactions used for the services being rendered through the Customer's account.
- e. connected accounts, if any.
- f. concerning specific transactions:
 - the origin of the funds

Carletta N.V. – Anti-Money Laundering Compliance Policy

- the type and amount of the currency involved in the transaction
- the form in which the funds were placed or withdrawn, for example, cash, cheques, wire transfers
- the identity of the person that gave the order for the transaction
- the destination of the funds
- the form of instructions and authorization that have been given
- the type and identifying number of any account involved in the transaction
- any other information which is available and deemed to be essential to the investigation

The Compliance Officer shall perform the following activities:

- Receive and investigate information from the Company's employees on unusual transactions that create the belief or suspicion of money laundering. This information is reported in the ISR or any other form that may be deemed appropriate from time to time by the urgency and severity of the situation. The said reports are archived by the Compliance Officer.
- Evaluate and check the information received from the employees of the Company, concerning other available sources of information and the exchanging of information concerning the specific case with the reporter and, where this is deemed necessary, with the reporter's supervisors. The information which is contained in the report which is submitted to the Compliance Officer is evaluated based on the ISR, being the basis for investigation. Such report is used by the Compliance Officer to record investigative steps, internal findings, and the final decision regarding submission to the FIU.
- If, because of the evaluation described above, the Compliance Officer decides to disclose this information to the FIU, then he prepares a written report, which he submits to the FIU.
- If because of the evaluation described above, the Compliance Officer decides not to disclose the relevant information to the FIU, then he fully explains the reasons for his decision and attaches to the initial ISR.
- To act as a first point of contact with the FIU, upon commencement of and during an investigation because of filing a report to the FIU according as indicated above.
- To maintain a registry that includes the reports of unusual transactions, and relevant statistical information (e.g. the department that submitted the internal report, date of submission to the Compliance Officer, date of assessment, date of reporting to the FIU), the evaluation reports and all the documents that verify the accomplishment of his duties.

6.9. AML Compliance Program

Carletta N.V. maintains a comprehensive AML Compliance Program designed to ensure effective oversight, implementation, and continuous improvement of its AML/CFT framework. The program includes structured responsibilities, clear procedures, training, screening, and

independent audit, as required under Chapter V.4–V.5 of the CGA AML/CFT Policy.

Component	Description	Reference
Internal Policies, Procedures, and Controls	The Company maintains documented AML/CFT procedures that define workflows, escalation protocols, and segregation of duties. Each process is mapped to internal controls.	Annex A
Compliance Function Structure	The Compliance Officer is responsible for daily AML oversight, policy updates, CRA validation, and escalation of ISR reports. Supporting roles are outlined in control sections.	Section 7 Annex H
Employee Screening Program	All AML-relevant staff are screened pre-employment and every 24 months. Screening includes ID, references, and qualification review. The full employee screening program is provided in Annex G.	Annex G
Employee Training Program	Role-based AML/CFT training is delivered at onboarding, annually, and upon regulatory changes. Content covers legal obligations, internal procedures, and red flags.	Annex E
Independent Audit and Testing	Carletta N.V. engages an independent auditor or external contractor on a competitive basis to test the AML/CFT Program annually. Selection is based on the candidate's expertise, professional certifications, and recognized qualifications in the field of AML/CFT compliance. The audit scope includes CRA/EDD validation, ISR/goAML handling, control testing, and a review of internal training and documentation procedures.	Section 6.11
Examinations by the Curaçao Gaming Authority	When under examination by and upon CGA's requests during the year, Carletta shall provide information or documentation on its AML/CFT/CFP policies and deterrence and detection procedures.	Section 6.12

6.10. Record keeping and monitoring

The Company shall maintain records of the Customer identification documents obtained during the Customer identification and applied due diligence procedures, as well as all necessary records on transactions (both domestic and international) for compliance with information requests from

Carletta N.V. – Anti-Money Laundering Compliance Policy

the competent authorities. Such records shall be sufficient to permit the 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.

The documents/data mentioned above shall be kept for at least five (5) years, which is to start running either from the termination of a business relationship or from the date on which an occasional transaction has been executed.

At the instruction of the FIU, the documents/data mentioned above that may be relevant to ongoing investigations shall be kept by the Company for up to ten (10) years or until the FIU confirms that the investigation has been completed and the case has been closed, whichever comes first.

Furthermore, should the firm require the documents for the institution, prosecution or to defend against any claim for which a longer prescriptive period exists, then such records will be kept until the claim is extinguished or such prescriptive period has elapsed.

6.11. Independent audit

Carletta N.V. maintains an independent audit function as part of its AML/CFT Compliance Program in line with Chapter V.5 of the CGA AML/CFT Policy. The purpose of the independent audit is to assess the effectiveness of the Company's AML policies, procedures, controls, and operational execution.

The audit is performed annually or more frequently if required by material changes in operations, regulatory requirements, or internal risk findings. The audit may be conducted by the Internal Auditor or an external, independent contractor selected on a competitive basis. The selection criteria for external providers include:

- Proven expertise in AML/CFT auditing;
- Professional certifications (e.g., CAMS, ICA);
- Relevant jurisdictional or regulatory accreditation;
- Independence from Carletta N.V.'s day-to-day operations.

The audit scope includes, but is not limited to:

- An evaluation of the Carletta's AML/CFT/CFP manuals;
- Customers file review;
- Compliance management;
- Performance of transaction testing;
- Adequacy of employee training and awareness;
- Assessment of compliance with applicable laws and regulations;

- Evaluation of the system's ability to identify unusual activity;
- Interviews with employees who handle transactions and with their supervisors;
- A sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements;
- An assessment of the adequacy of the record retention system; and
- An assessment of the Company's responsiveness to earlier audit findings.

Findings are compiled into an Audit Report, which is submitted to Senior Management with recommendations and corrective actions. Audit results are reviewed and acted upon within pre-determined deadlines. Audit reports are maintained for a minimum of five years and are available to regulators upon request.

6.12. Examination by the Curaçao Gaming Authority (CGA)

In accordance with Chapter V.6 of the CGA AML/CFT Policy, Carletta shall provide information or documentation on its AML/CFT/CFP policies and deterrence and detection procedures to the examiners of the CGA in preparation of or during an examination and upon CGA's requests during the year.

The following items shall be made readily available:

- The written and approved AML/CFT/CFP compliance program;
- Records of its Business Risk Assessment (BRA);
- The name of each Compliance Officer responsible for Carletta's overall AML/CFT/CFP policies and procedures and his/her designated job description;
- Records of UTRs;
- Records of unusual transactions that required closer investigations;
- Records of frozen accounts;
- Schedule of ML/FT/FP training provided to Carletta's employees;
- The assessment report on Carletta's AML/CFT/CFP policies and procedures by the internal audit department or an external auditor;
- Customers' files, including Customer Risk Assessment, CDD, customer acceptance and transaction information.

7. AML GOVERNANCE & RESPONSIBILITIES

Current legislation enforces Customer Due Diligence on transactions, and having this process in place, has made such activity harder for those intent on laundering money generated from illegal activities. It is of utmost importance to the Company that the policies and procedures are structured in a way that ensures compliance with regulators and legal frameworks, ensuring that the Company

Carletta N.V. – Anti-Money Laundering Compliance Policy

is not an attractive vehicle for terrorist financing.

The Company's AML and CTF policies, procedures, and internal controls are designed to ensure compliance with all applicable legislation and best practice procedures. The policies are reviewed and updated regularly to ensure all applicable procedures and internal controls are up to date to account for both changes in regulation and internal changes that could present new risk factors.

The following departments are directly targeted by the requirements of this procedure:

Board of Directors – Approval and Signature requirements, especially in high-risk scenarios, availability of sufficient resources for AML compliance.

All Key Functions – Knowledge of procedure and understanding of requirements.

Customer Support – Understanding of onboarding and reporting requirements.

KYC Department – Understanding and applying DD requirements.

Security – Understanding DD requirements.

Fraud – Understanding the difference between a fraud case and an ML case.

Finance Department – Understanding the risks posed by ML/TF/FP (Refer to Chapter 7).

Legal Department – Ensuring all legislative requirements are met.

Compliance Officer – Refer to the CGA Requirements for Compliance Officer Based on NOIS/NORUT included in **Annex H**.

All Key Functions (including Customer Support, KYC Provider, Antifraud, Finance, and Legal when applicable) collectively form part of the First Line of Defense and are responsible for applying and executing AML/CFT controls within their business operations. The scope of this procedure may be extended to other departments if the need ever arises and all employees need to be attentive and aware of the information flow regarding the prevention of money laundering and funding of terrorism and proliferation of weapons of mass destruction.

The functional responsibilities of departments and personnel involved in AML/CFT implementation are further illustrated in the Company's Three Lines of Defense structure presented in **Annex A** of this Policy.

The Compliance Officer shall belong hierarchically to the management level of the Company's organizational structure to command the necessary authority. Furthermore, the Compliance Officer shall lead the Company's Money Laundering Compliance procedures and processes and report to the Senior Management. The Compliance Officer shall also have access to all relevant information necessary to perform his duties. The level of remuneration of the Compliance Officer shall not compromise his objectivity.

The legally prescribed responsibilities of the Compliance Officer are included in **Annex H - Responsibilities of the Compliance Officer as required by the CGA**. In addition, within the

Company it is the Compliance Officer's responsibility:

- To ensure the preparation and maintenance of the lists of Customers categorized following a risk-based approach, which contains, among others, the names of Customers, their account numbers, and the dates of the commencement of the Business Relationship. Moreover, the Compliance Officer ensures the updating of the said list with all new or existing Customers, in the light of any additional information obtained.
- To detect, record, and evaluate, at least on an annual basis, or on the happening of any event which might have an impact on the overall risk, all risks arising from existing and new Customers, new financial instruments and services, and update and amend the systems and procedures applied by the Company for the effective management of the aforesaid risks should it be required and appropriate to do so.
- To evaluate the systems and procedures applied by a third party with whom the Company has entered into a reliance agreement in terms of Customer Due Diligence including Customer Identification and Verification of the Customer, Identification & Verification of Beneficial Owners as well as the Purpose & Intended Nature of the Business Relationship applied and approves the cooperation with such third parties.
- To ensure that all the branches and subsidiaries of the Company, if any, have taken all necessary measures for achieving full compliance with the provisions of the Anti-Money Laundering Compliance Policy, concerning Customer identification, due diligence, and record-keeping procedures.
- To provide advice and guidance to the employees of the Company on subjects related to money laundering and terrorist financing.
- To acquire the knowledge and skills required for the improvement of the appropriate procedures for recognizing, preventing, and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing.
- To determine whether the Company's departments and employees require further training and education for preventing Money Laundering and Terrorist Financing and organizing appropriate training sessions/seminars. In this respect, the Compliance Officer shall prepare and apply an annual staff training program. Also, the Compliance Officer assesses the adequacy of the education and training provided.
- To prepare the Annual Report, as required by the FIU and any other applicable authority.
- To respond to all requests and queries from the FIU, provide all requested information and fully cooperate with the FIU, if required.
- To maintain a registry that includes the reports of unusual transactions, and relevant statistical information (e.g. the department that submitted the internal report, date of submission to the Compliance Officer, date of assessment, date of reporting to the FIU), the evaluation reports and all the documents that verify the accomplishment of his duties.
- To review the Customer's files and to approve or reject prospective High-Risk Customers.

Carletta N.V. – Anti-Money Laundering Compliance Policy

- To develop and establish the Customer Acceptance Policy and submit it to the Senior Management for consideration and approval.
- To review and update the Anti-Money Laundering Compliance Policy as may be required from time to time, and for such updates to be communicated to the Senior Management for their approval, at least annually or at any such period as may be deemed necessary by the Compliance Officer.
- To monitor and assess the correct and effective implementation of the policy practices, measures, procedures, and controls and in general the implementation of the Anti-Money Laundering Compliance Policy. In this respect, the Compliance Officer shall apply appropriate monitoring mechanisms (e.g. on-site visits to different departments of the Company) which will provide him with all the necessary information for assessing the level of compliance of the departments and employees of the Company with the procedures and controls which are in force. If the Compliance Officer identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures, and controls, shall give appropriate guidance for corrective measures and where deemed necessary to inform the Senior Management.

The Financial Department Management and staff are responsible for monitoring all transactions to and from the Company and verifying the identity of all online registered Players requesting a withdrawal, who have reached the XCG 4,000. They must also establish parameters by which any suspicious activity can be immediately noted, and form procedures by which to solve these issues while keeping the risk to a minimum. Such staff must follow the guidelines and requirements as per the Kingdom Sanctions Act, NOIS, NORUT, Sanction National Ordinance, Regulations, EU Directives on the Prevention of Money Laundering and Funding of Terrorism, and any other applicable laws and regulations.

The above-mentioned regulations require obliged entities to verify the Player in such a way that the source of funds is also identified. The verification process will be documented in such a way that every Player will have a risk profile, and file, and, if any Unusual Transaction Report needs to be filed, all evidence in respect of the Player will be on hand.

Carletta N.V. maintains a structured internal control framework aligned with the Three Lines of Defense model (as defined in **Annex A – Three Lines of Defense**). Internal controls are implemented proportionately to customer risk and are designed to ensure effective prevention, detection, escalation, and reporting of ML/TF risks.

Key elements include:

- Clear separation of duties between business units, the Compliance Officer, and the Internal Auditor;
- Four levels of risk-based control applied to customer accounts, based on CRA

- classification;
- Pre-defined escalation paths for risk events (see Section 6);
- Integration of automated and manual control measures (e.g., transaction limits, device monitoring);
- Oversight from the Compliance Officer and periodic review of control effectiveness.

Roles within the first line of defense, including the KYC Provider and operational teams, are supported by procedures in **Annex A – Three Lines of Defense**.

8. EMPLOYEE TRAINING PROGRAM

The Company shall ensure that training and updates are provided to employees and key people involved in the prevention of AML and fraud within the Company. Such training may be in-house or from third-party providers. All training provided shall be in line with and in proportion to the roles and duties of the individual employee. Training shall be tailored to the tasks and duties of the employee and the Company shall not adopt a one size fits all approach. Training shall be provided regularly and when needed. However, a yearly refresher course shall be provided to ensure that all employees are up to date on recent developments.

Records of such training received shall be kept on file as proof of attendance in such training.

8.1. Employees' obligations

- (a) The Company's employees shall be personally liable for failure to report any information relating to knowledge or suspicion, regarding money laundering or terrorist financing.
- (b) the employees must cooperate and report internally, without delay, and by not later than 24 hours, anything that comes to their attention concerning transactions for which there are grounds for suspicion that the person is involved in money laundering or terrorist financing.
- (c) according to the applicable Law, the Company's employees shall fulfill their legal obligation to report their suspicions regarding Money Laundering and Terrorist Financing, after they comply with point (b) above.

8.2. Employees' Education and Training

- (a) The Compliance Officer shall ensure that the employees are fully aware of their legal obligations according to the applicable Laws, regulations, directives, and implementing procedures by introducing an ongoing employee education and training program.
- (b) The timing and content of the training provided to the employees of the various departments will be determined according to the needs of the Company. The frequency of the training can

Carletta N.V. – Anti-Money Laundering Compliance Policy

vary depending on the amendments to legal and/or regulatory requirements, employees' duties as well as any other changes in the system of Curaçao.

- (c) the training program aims to educate the Company's employees on the latest developments in the prevention of Money Laundering and Terrorist Financing, including the practical methods and trends used for this purpose.
- (d) the training program will have a different structure for new employees, existing employees, and different departments of the Company according to the services that they provide.
- (e) On-going training shall be given at regular intervals to ensure that the employees are reminded of their duties and responsibilities and kept informed of any new developments.

The Compliance Officer shall ensure that records of the Company's employee training program, including participation and content, are maintained and summarized in internal compliance reporting.

Refer to **Annex I – Ongoing Employee Training Program** for more details.

8.3. Compliance Officer Education and Training Program

The Compliance Officer shall be responsible for any updates to the Law and attend any external training necessary. Based on his/her training the Compliance Officer will then provide training to the employees of the Company.

The main purpose of the Compliance Officer training is to ensure that relevant employee(s) become aware of:

- the Law and the Regulations
- the Company's Anti-Money Laundering Policy
- the statutory obligations of the Company to report unusual transactions
- the employee's own personal obligation to refrain from activity that would result in money laundering
- the importance of the Customers' due diligence and identification measures requirements for money laundering prevention purposes.

The Compliance Officer shall document his or her own participation in relevant AML/CFT training and ensure that such information is available to Senior Management and, where applicable, included in compliance reporting and oversight materials.

9. CONSEQUENCE OF NON-COMPLIANCE (NOIS and NORUT)

Under the National Ordinance on the Identification when rendering Services (NOIS) and the National Ordinance on the Reporting of Unusual Transactions (NORUT), failure to comply with AML/CFT obligations may result in significant legal consequences for the Company and its responsible officers.

9.1. Sanctions for Non-Compliance

- Administrative fines imposed by the supervisory authorities;
- Criminal sanctions, including imprisonment, for willful or grossly negligent breaches;
- Revocation of licenses or regulatory permissions issued by the Curaçao Gaming Authority (CGA);
- Public naming and reputational damage via enforcement disclosures.

9.2. Personal Liability of Responsible Officers

Company officers, directors, and senior management may be held personally liable for:

- Failure to implement or enforce adequate AML/CFT procedures;
- Failure to report unusual transactions within the required timeframe;
- Knowingly or negligently ignoring unusual activity of Players;
- Engaging in or facilitating tipping-off.

In accordance with Curaçao law, such breaches may lead to civil, administrative, or criminal penalties, depending on severity and intent.

The Company ensures that all relevant personnel are trained on these obligations and that responsibilities under NOIS/NORUT are clearly defined and documented.

10. AGENTS/INTERMEDIARIES

The Company shall be responsible for creating and maintaining its customer base, and, for the foreseeable future, shall not engage any intermediaries or Agents nor shall it accept Customers coming from such individuals or entities. Should the Company decide to change its policy on the above, a more detailed policy is to be created and approved by the Board of Directors, highlighting how such entities will be handled in line with the applicable legislation and regulation at that time. Introducers, such as affiliates, do not fall within such category as their role is to merely introduce the Customer to the Company and will have no further involvement in the business relationship.

11. RELATED INFORMATION

Carletta N.V. – Anti-Money Laundering Compliance Policy

This Policy should be read in conjunction with:

- CGA AML/CFT Policy (January 2025);
- National Ordinance on the Reporting of Unusual Transactions (NORUT);
- Ministerial Decree Indicators Unusual Transactions (N.G. 2015 no. 73)
- National Ordinance on the Identification when rendering Services (NOIS);
- FATF 40 Recommendations;
- Kingdom Sanctions Act (Rijkssanctiewet);
- goAML Portal & Reporting Guidelines;
- Transparency International Corruption Perceptions Index (CPI);
- **Annex A – Internal Control Structure: Three Lines of Defense**
- **Annex B – Trigger-Based Risk Scoring Table**
- **Annex C – Jurisdiction Risk Classification and Prohibited Countries List**
- **Annex D – Internal Suspicion Report Form (ISR)**
- **Annex E – AML/CFT Training Plan**
- **Annex F – Examples of Unusual Transactions**
- **Annex G – Employee Screening Program**
- **Annex H - Responsibilities of the Compliance Officer as required by the CGA**
- **Annex I – Ongoing employee training program**

12. CONTACT INFORMATION

For questions, compliance support, or to report suspicious activity, please contact:

Compliance Department

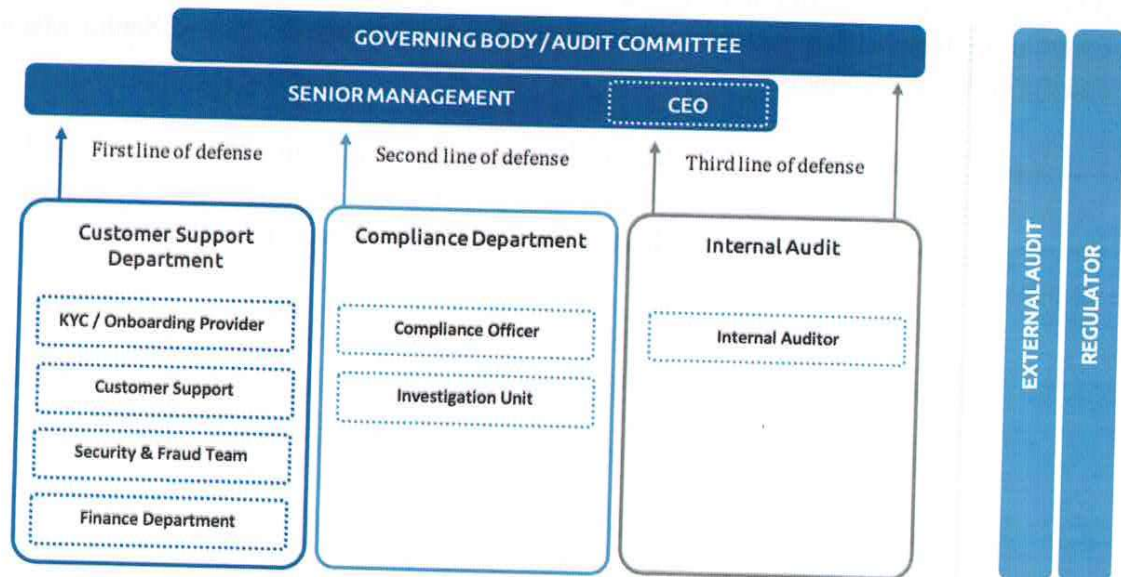
Carletta N.V.

Email: finance@pin-up.team

Phone: +447458197085

ANNEX A - Internal Control Structure: Three Lines of Defense

This diagram below illustrates the Company's Three Lines of Defense model, which defines the allocation of roles and responsibilities in the prevention of money laundering, terrorist financing, and proliferation of weapons of mass destruction and other financial crimes.



First Line of Defense – Operational Functions

The first line of defense is composed of all operational departments and service providers directly involved in Customer interaction and transaction processing. This includes the KYC/Onboarding Provider, Customer Support, Fraud and Security Team, and the Finance Department. These units are responsible for applying due diligence measures, performing ongoing monitoring, and detecting potentially unusual or suspicious activity during day-to-day operations.

Second Line of Defense – Compliance Oversight

The Compliance Department acts as the second line of defense by providing independent oversight, developing and maintaining the AML/CFT framework, and reviewing alerts or escalations from the first line. The Compliance Officer and Investigation Unit (usually lawyer's team) assess whether activities or transactions meet the threshold for reporting to the FIU and ensure the ongoing adequacy of AML controls.

Carletta N.V. – Anti-Money Laundering Compliance Policy

Third Line of Defense – Internal Audit

The third line of defense provides independent assurance of the effectiveness of the Company's AML/CFT Policy. The Internal Auditor evaluates the design and operational effectiveness of the controls implemented by the first and second lines, and reports findings to Senior Management and the Governing Body.

Oversight from the Governing Body / Audit Committee and Senior Management, including the CEO, ensures strategic supervision, resource allocation, and accountability. The Company also remains subject to independent evaluation by External Audit and regulatory supervision by the Regulator.

ANNEX B - Trigger-Based Risk Scoring Table

The table below includes a detailed list of risk triggers categorized by type, along with example behaviors and the associated numerical score used within the Company's AML risk scoring model. These triggers support dynamic risk reassessment and guide the application of due diligence measures.

The trigger-based scoring model used in the CRA derives directly from the Company's Business Risk Assessment (BRA). Each operational trigger listed in Annex B is based on a risk factor that was prioritized in the BRA based on its likelihood and impact.

These prioritized risks are translated into Customer-facing triggers (e.g., structuring, use of VPN, forged ID) and assigned normalized scores (1–3) depending on their relevance and severity. Each such trigger contributes to the Customer Risk Score, supports dynamic reassessment, and may initiate Enhanced Due Diligence (EDD) or an Unusual Transaction Report (UTR) where warranted.

Risk Category	Trigger Description	Example Behavior / Detection	Risk Score
Customer	Multiple accounts from same device	Same device ID used across 2+ user accounts	2
Customer	Refusal to provide SoF	Customer declines to submit source of funds documentation when required during withdrawal or EDD	3
Customer	Unverified or forged documents	Submitted ID has visual anomalies or fails document integrity check	3
Customer	False occupation or inconsistent profile	Declared profession (e.g. student) does not match transaction volume	2
Geographic	Use of VPN or proxy	Login IP address linked to VPN service or shows rapid country switching	2

Carletta N.V. – Anti-Money Laundering Compliance Policy

Risk Category	Trigger Description	Example Behavior / Detection	Risk Score
Geographic	Access from high-risk country	Login or deposit from jurisdiction on FATF blacklist or grey list	3
Geographic	Geolocation mismatch	Deposit from one country, access from another (e.g., card: DE, IP: RU)	3
Product	Fast withdrawal without gameplay	Deposit followed by immediate withdrawal request without wagering	2
Product	Bonus abuse pattern	Multiple bonuses claimed in short period with minimal qualifying activity	2
Product	High-value single game payout	Unusually large win in low-variance game immediately followed by withdrawal	2
Delivery	Third-party payment method	Cardholder name differs from account holder	1
Delivery	Unregulated or anonymous PSP	Deposit via crypto/PSP without license or transparent ownership	3
Delivery	Frequent changes in payment method	User adds/removes 3+ payment methods within 7 days	3
Behavior	Structuring	Multiple small deposits (e.g., XCG 3,900) just below threshold to avoid SoF trigger	3
Behavior	Churning activity	Frequent deposits and withdrawals with limited or no gameplay	3
Behavior	High-frequency failed deposits	User initiates 5+ failed deposits within 24 hours	2

Carletta N.V. – Anti-Money Laundering Compliance Policy

Risk Category	Trigger Description	Example Behavior / Detection	Risk Score
Behavior	Rapid turnover post-KYC	Account dormant, then sudden surge in activity right after ID approval	2
Behavior	Withdrawals to new methods	User changes payment method immediately before withdrawal request	3

ANNEX C - Jurisdiction Risk Classification and Prohibited Countries List

This annex outlines the Company's framework for classifying jurisdictions according to geographical risk. This classification supports onboarding decisions, ongoing customer due diligence (CDD), and monitoring, in line with a risk-based approach under Curaçao AML/CFT regulations.

Countries are grouped into four categories based on regulatory prohibitions, international AML/CFT evaluations, and governance risk indicators.

1. Prohibited Jurisdictions

These are jurisdictions from which the Company will not accept Customer traffic or registrations under any circumstances. Players attempting to register from these jurisdictions must be automatically blocked. Access must be technically restricted and actively monitored.

This includes:

- Countries subject to comprehensive international sanctions or embargoes.

Please follow these links for the most updated lists:

UN Sanctions List: <https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>

EU Sanctions List: <http://www.sanctionsmap.eu/#/main>

- Other countries prohibited as per Company policy.

List of other jurisdictions prohibited as per Company policy

Australia. France and its territories. Hong Kong. Italy. Netherlands and its territories (Curacao, Aruba, Bonaire, Saba, Sint Maarten, St. Eustatius).	Singapore. Spain. United Kingdom of Great Britain and Northern Ireland. United States of America.
---	--

Depending on global developments, this list may change from time to time.

2. High-Risk Jurisdictions

These jurisdictions (excluding already prohibited countries) may be accepted only with enhanced due diligence (EDD) and require explicit approval by the Compliance Officer. This group includes:

- Countries listed by the Financial Action Task Force (FATF) as:
 - High-Risk Jurisdictions Subject to a Call for Action, and
 - Jurisdictions Under Increased Monitoring.

Please follow the link to the most updated FATF-lists:

<https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html>

- CFATF Public Statements

Please follow the link to the CFATF Public Statements:

<https://www.cfatf-gafic.org/home/public-statements>

- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State annual International Narcotics Control Strategy Report (INCSR)

Please follow the link to the International Narcotics Control Strategy Reports:

<https://www.state.gov/international-narcotics-control-strategy-reports/>

- Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime

Please follow the link to the EU list of high-risk third countries:

https://eur-lex.europa.eu/eli/reg_del/2016/1675

- Countries identified by OFAC as presenting elevated financial crime or sanctions risk.

Please follow the link to the most updated OFAC-lists:

<https://sanctionslist.ofac.treas.gov/Home/SdnList>

- Jurisdictions, demonstrating higher exposure to corruption, weak institutions, or political instability, based primarily on the Transparency International Corruption Perceptions Index (CPI). A CPI-range of 0-40 is considered high risk.

Please follow the link to the most recent CPI:

<https://www.transparency.org/en/cpi/2024>

3. Medium-Risk Jurisdictions

Jurisdictions not under sanctions but demonstrating higher exposure to corruption, weak institutions, or political instability, based primarily on the Transparency International Corruption Perceptions Index (CPI). A CPI-range of 41-70 is considered medium risk. EDD may be applied at the discretion of the Compliance Officer.

Please follow the link to the most recent CPI:

<https://www.transparency.org/en/cpi/2024>

4. Standard-Risk Jurisdictions

All jurisdictions not included in the above categories fall under standard risk. Customers from these countries are subject to regular CDD and monitoring unless elevated risks are identified during the Customer risk assessment.

Important Notes

- This classification supports but does not replace individual Customer risk assessments.
- This annex must be reviewed at least annually, and updated when international risk assessments or CGA/ FIU notifications change.
- Customers from high- or medium-risk jurisdictions may still be rejected if other risk factors apply.

Clarification on UNSC Sanctions

The United Nations Security Council (UNSC) Consolidated Sanctions List contains individuals, entities, and groups subject to international sanctions.

It is not a country-level risk classification tool and is therefore not included in this annex. However, screening against the UNSC list is mandatory for all Customers and is handled separately as part of the Sanctions List Screening procedure described in the main AML Compliance Policy.

ANNEX D - Standardized template of the Internal Suspicion Report (ISR)

This establishes the form of report that the Employee must fill in and forward to the Compliance Officer in cases specified in Anti-Money Laundering Compliance Policy. The Compliance Officer must accept the report, and the documents attached to it and consider the need to send a notification to the competent authority or, if necessary, perform other activities.

1. Employee Information • Name of employee submitting the report: • Department / Role: • Date and time of report submission:	
2. Customer Information • Full name of the customer: • Date of birth / National ID or player account number: • Customer jurisdiction (residency or activity location):	
3. Transaction or Behavior Description • Date and time of transaction or behavior: • Amount involved (if applicable): • Description of transaction or unusual activity:	
4. Grounds for Suspicion • Description of trigger or reason for concern: (e.g., structuring, unusual deposit pattern, forged document, excessive withdrawals, etc.) • Type of risk identified: ☐ Money Laundering ☐ Terrorist Financing ☐ Other (please specify): _____	

Carletta N.V. – Anti-Money Laundering Compliance Policy

5. Supporting Documents Attached • ☐ Transaction records • ☐ Chat/email transcripts • ☐ ID documents • ☐ Payment method records • ☐ Other (describe): _____	
6. Compliance Officer Review Section (to be completed by the Compliance Officer) • Date of internal report received: • Actions taken (e.g., transaction analysis, pattern review, SoF/SoW checks, request to bank): • Outcome of internal investigation: ☐ No further action ☐ Ongoing monitoring ☐ UTR submitted via goAML • Date of UTR submission (if applicable): • Reference number of goAML submission: • Notes:	

ANNEX E - Annual AML/CFT Training Plan

This annex outlines the structured training framework adopted by Carletta N.V. for AML/CFT compliance, in accordance with Curaçao AML/CFT Regulations, the Sanctions National Ordinance, and CGA regulatory expectations. The training program ensures that all relevant staff are aware of their obligations under the AML/CFT regime, and are equipped to detect, assess, and escalate ML/TF/FP risks.

1. Objective

To ensure that all employees, contractors, and relevant third-party service providers receive tailored, role-specific training on AML/CFT compliance. Training supports effective implementation of the Company's internal controls, Customer Acceptance Policy (CAP), and goAML reporting obligations.

2. Training Audience and Frequency

- Compliance Officer – Annual, and following material regulatory changes
- Senior Management – Annual
- KYC Provider (KYCAID LIMITED) – Annual
- Customer Support and Payment Staff – Bi-Annual
- Fraud, Risk, and Monitoring Teams – Quarterly
- New Employees – Upon hiring

3. Training Topics

- Curaçao AML/CFT legal framework (NOIS, NORUT, CGA regulations)
- Identifying and reporting unusual transactions
- Using the Internal Suspicion Reporting (ISR) Form
- Escalation process: from detection to goAML reporting
- Sanctions screening procedures and PEP handling
- Customer Risk Assessment (CRA) methodology and red flags
- Practical case studies and simulation of UTR submission

4. Delivery Methods

Training shall be delivered using a blended approach:

- Online modules and case-based quizzes
- Live webinars and instructor-led sessions

Carletta N.V. – Anti-Money Laundering Compliance Policy

- Periodic knowledge assessments
- Internal memos and policy update briefings

5. Records and Evaluation

Attendance logs, completion certificates, and training results will be maintained by the Compliance Officer. Effectiveness of training will be reviewed annually and adjustments made to address evolving risks.

ANNEX F - Examples of unusual transactions/activities related to money laundering and terrorist financing

Money laundering

Under the laws of multiple jurisdictions, money laundering is a serious offense. Money laundering involves various acts committed to conceal or convert property or the proceeds derived from such property (such as money) knowing or believing that these were derived from the commission of a designated offense. In this context, a designated offense means an offense under the Criminal Code (Title XXXI of the Penal Code of Curaçao) or any other applicable law or the equivalent law in the jurisdiction within which such offense has or is suspected to have taken place. It includes but is not limited to those offenses relating to illegal drug trafficking, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation, tax evasion, and copyright infringement amongst others.

Unusual transactions are financial transactions that you have reasonable grounds to suspect are related to the commission of a money laundering offense. This includes transactions that you have reasonable grounds to suspect are related to the attempted commission of a money laundering offense.

“Reasonable grounds to suspect” is determined by what is reasonable in your circumstances, including normal business practices and systems within the industry. While NORUT and Regulations do not specifically require the Company to implement or use an automated system for detecting unusual transactions, we do have such a system in place.

In this context, “transactions” include both completed and attempted transactions, as previously defined. The Company’s compliance framework incorporates a continuous risk assessment process aimed at identifying potential money laundering or terrorist financing threats. In higher-risk situations, the Company applies enhanced ongoing monitoring measures to ensure that suspicious behavior or patterns are promptly detected, investigated, and, where appropriate, reported to the FIU.

Completed transactions

A completed transaction refers to any financial transaction that has been successfully executed by or on behalf of the Customer. This includes, for example, deposit, wagering, and withdrawal transactions. Even if the Customer requests a withdrawal of unspent funds, such an action is still considered a completed transaction and may fall within the scope of AML monitoring procedures if it appears inconsistent with the Customer’s known profile or expected behavior.

Attempted transactions

An attempted transaction is one that a Customer intended to conduct and took some form of action to do so. An attempted transaction is different from a simple request for information, such as an inquiry as to the fee applicable to a certain transaction. An attempted transaction includes entering negotiations or discussions to conduct the transaction and involves concrete measures to be taken by either you or the Customer. A formal request by the Customer to withdraw funds from their account would constitute such an attempt.

The following are examples of attempted transactions:

- A financial entity or casino refuses to accept a deposit because the Customer refuses to provide identification as requested.
- A securities dealer or life insurance agent refuses to process a transaction - for which the Customer insists on using cash - because their business practice is not to accept cash.
- A Customer of a real estate agent starts to make an offer on the purchase of a house with a large deposit but will not finalize the offer once asked to provide identification.
- An individual asks an accountant to facilitate a financial transaction involving large amounts of cash. The accountant declines to conduct the transaction.
- A money services business will not process a request to transfer a large amount of funds because the Customer requesting the transfer refuses to provide the identification requested.

To report an attempted transaction, it must be one that you have reasonable grounds to suspect that it is related to money laundering or terrorist financing. An attempt to conduct a transaction does not necessarily mean the transaction is suspicious/unusual. However, the circumstances surrounding it might contribute to your having reasonable grounds for suspicion.

Transactions related to terrorist property

In line with Curaçao AML/CFT Regulations and the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Company monitors for activity that may indicate attempted or completed transactions involving terrorist property or the financing of terrorism. While such transactions may not always be clearly labeled as terrorist-related, the following patterns may give rise to suspicion and warrant immediate escalation to the Compliance Officer. The following are examples of red flags that may indicate such risks. This list is non-exhaustive, and other circumstances may also be deemed by the Company to constitute transactions related to terrorist property or terrorist financing, based on the context, available information, and risk assessment:

1. Unusual use of foreign or high-risk payment instruments: use of prepaid, business, or third-party cards not consistent with the Player's declared profile or country; use of payment

methods originating from or linked to jurisdictions known for terrorist financing risks or FATF high-risk classification.

2. Anonymity and account layering behavior: frequent switching of devices or accounts with overlapping attributes (e.g., same IP, same device ID); multiple accounts linked to similar addresses, payment methods, or devices—indicating possible use of mules or proxies.
3. Suspicious deposit and withdrawal behavior: large deposits made with no gameplay or minimal turnover, followed by withdrawal requests; structuring of transactions to avoid detection (e.g., multiple deposits just under risk threshold); attempt to withdraw funds to newly added payment methods or accounts not previously verified. No meaningful gaming activity between deposit and withdrawal (pure money movement).
4. Geographic and identity inconsistencies: accounts accessed from or funded via countries with elevated TF risks, using VPNs or proxies; discrepancies between declared personal details and the geographic origin of funds or access points.
5. Behavior that indicates possible channeling of funds: use of gaming accounts solely for deposit and withdrawal cycles without genuine gaming activity; repeated cancellation of bets or unusual in/out flows inconsistent with the Customer's risk profile.
6. Use of high-risk payment providers: use of lesser-known, offshore, or unlicensed PSPs (Payment Service Providers), especially those operating without clear KYC obligations; known facilitation of anonymous funding (e.g., crypto-fiat mixers, cash-funded prepaid vouchers).
7. Unusual behavior such as the cancellation of a withdrawal shortly after submission, particularly following account verification or bonus fulfillment, may warrant further investigation.
8. A Player is unwilling to provide sufficient or accurate information during onboarding or enhanced due diligence, including the purpose of using the gaming account, expected transaction behavior, or the source of funds and source of wealth. The information submitted may appear minimal, vague, or unverifiable, raising concerns regarding the legitimacy or transparency of the Player's profile.
9. A Player provides identification documents that raise concerns due to poor quality, inconsistencies, or lack of verifiability, which may indicate an attempt to conceal true identity or avoid proper due diligence.
10. A Player fails to provide required verification documents in a timely manner, or repeatedly submits incomplete or inconsistent documentation, potentially indicating an attempt to avoid proper due diligence.
11. Unexplained inconsistencies arising during the process of identifying and verifying the Customer (e.g. previous or current country of residence, country of issue of the passport, countries visited according to the passport, documents furnished to confirm name, address, and date of birth, etc.).

ANNEX G - Employee screening program

All employees and contractors assigned to AML/CFT-relevant roles must undergo a documented screening process before being granted access to AML-related functions.

Scope of Screening

- Identity verification (government-issued ID);
- Employment reference checks;
- Verification of qualifications relevant to the role;
- Screening against internal watchlists and external sanctions lists;
- Confirmation of clean disciplinary and criminal background (where allowed by law).

Ongoing Screening

- Re-screening occurs at least once every 24 months;
- Additional screening is required upon promotion, transfer to sensitive roles, or performance-related incidents.

Screening outcomes are documented and maintained by the Compliance Department and may be shared with management upon request.

ANNEX H - Responsibilities of the Compliance Officer as required by the CGA⁴

5. Scope of Responsibilities

The operator must formally designate a senior officer at the management level as responsible for detecting and deterring money laundering and terrorist financing. This AML/CFT Compliance Officer should have timely access to customer identification data, Customer Due Diligence (CDD) information, transaction records, and other relevant data, and must be able to act independently.

The Compliance Officer is responsible for:

- Designing and implementing the AML program.
- Ensuring compliance with Curaçao laws and regulations regarding money laundering and terrorist financing.
- Reviewing adherence to the casino's policies and procedures.
- Organizing staff training sessions on compliance-related issues.
- Analyzing transactions and identifying those subject to reporting under the Ministerial Decree on Indicators for Unusual Transactions.
- Reviewing internally reported unusual transactions for completeness and accuracy.
- Maintaining records of both internally and externally reported unusual transactions.
- Design an internal procedure about when reporting of unusual transactions will lead to blocking/ freezing of user accounts
- Conducting further investigations into unusual transactions if necessary.
- Preparing external reports on unusual transactions.
- Making necessary changes to the AML program.
- Staying informed about local and international developments related to money laundering and terrorist financing and suggesting improvements to management.
- Preparing periodic reports on the casino's efforts against money laundering, terrorism financing, and proliferation financing.

⁴ GCB Requirements for Compliance Officer Based on NOIS/NORUT, implementation date January 1, 2025.

ANNEX I – Ongoing employee training program

In compliance with Chapter V.4 of the CGA AML/CFT Policy, the Company shall develop training programs and provides training to all personnel who handle transactions that may be qualified as unusual based on the indicators outlined in the Ministerial Decree Indicators Unusual Transactions (N.G. 2015 no. 73, as amended). Training includes setting out rules of conduct governing employee's behavior and their ongoing education to create awareness of the casino's policies against money laundering and terrorist financing. Most areas of the Company shall receive training and the target audience shall include most employees. Each segment shall be trained on topics and issues that are relevant to them.

Training must at least address the following topics:

a. New employees

- The nature and process of ML/FT/FP, specifically methods and trends in the Company's specific business line.
- The need to report any unusual transactions to the appropriate designated officer. Shall be provided to all new employees who will handle customers or their transactions, irrespective of their level of seniority.
- The existing internal policies, procedures and regulations concerning ML/FT/FP and the reporting requirements.
- CDD
- Objective and subjective indicators for UTRs.

b. Employees tasked with the first line of defense against ML/FT/FP

- The importance of AML/CFT/CFP, including some basics.
- ML/FT/FP typologies using online gaming companies.
- The Company's procedures to equip them to recognize potential ML/FT/FP and the actions to take.
- Personnel involved with account opening shall be made aware of the need to verify the identity of the customer.

c. Audit staff

These are employees charged with overseeing, monitoring and testing money laundering controls.

- Changes in regulation, money laundering methods and enforcement, and their impact on the organization.

d. AML/CFT/CFP Compliance staff

These are employees who run the AML program.

- Specialized training to stay on top of new trends or changes that impact the Company and the way it manages risk. This will require attending conferences or AML/CFT/CFP-specific presentations to go into greater detail.

e. Supervisors and Managers

Those tasked with the responsibility to supervise or manage the staff.

- A higher level of instruction covering all aspects of ML/FT/FP, procedures and regulations

f. Senior management and board of directors

Money laundering issues and dangers should be regularly and thoroughly communicated to Senior Management and Board to keep them aware of the reputational risk that money laundering poses to the Company.

Refreshment training

Refreshment training shall be arranged at regular intervals to ensure that employees are kept informed of current and new developments regarding ML/FT/FP techniques, methods and trends.

Record keeping

To demonstrate compliance with employee training guidelines, the Company shall maintain records that include:

- Details on the content of the training programs;
- The names of the employees who have received the training;
- The date on which the training was provided;
- The results of any testing carried out to measure employee understanding of ML/FT/FP requirements; and
- An ongoing training plan.

