

Green Forest Group N.V.

AML/CFT Procedures

Table of Contents

1.	Introduction and Objectives	3
1.1	What is the meaning of AML/CFT?	3
2.	Responsibilities	4
3.	Company Policy and Procedures.....	4
3.1	Suitability	4
3.2	Activation of Account	5
3.3	Know Your Customer	5
3.4	Players' Risk Levels.....	6
3.5	Verification based on Risk.....	7
3.6	Medium and High Risk Customers.....	8
4.	AML Procedures.....	8
4.1	Training Related to AML.....	9
4.2	Calculation of Risk.....	9
4.3	PEPs – Politically Exposed Persons	10
4.4	Risk Monitoring.....	11
4.5	Monitoring of Transactions – Customer Risk.....	11
4.6	Business Relation Obligation	12
4.7	Reporting of Transactions.....	13
4.1.1	Identification of Unusual Transactions.....	13
4.1.2	Documentation of Unusual Transactions	14
4.1.3	Reporting of Unusual Transactions	14
4.8	Record Keeping	15
5.	Employee Screening and Training	15
5.1	New Joiners.....	16
5.2	AML Compliance Team	16
5.3	Management	17
5.4	Training Program.....	17
6.	Consequences of non-Compliance	17
7.	Payout Management.....	18
7.1	Deposit Process	18
7.2	Withdrawal Process	18
7.3	Handling of Funds.....	19
8.	Contact Information.....	20

1. Introduction and Objectives

This document establishes a comprehensive framework for managing player settlements, authenticating player identities, and overseeing transactions to detect and deter fraudulent activities. It is designed to uphold the security and legitimacy of financial operations within the gaming platform.

Robust Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) measures play a pivotal role in protecting the financial infrastructure of the gaming sector. By implementing systems to identify, monitor, and prevent illegal financial behaviour—such as money laundering and the financing of terrorism—these measures reinforce the lawful operation of the platform.

Compliance with AML/CFT obligations also ensures adherence to the standards imposed by regulatory and financial oversight bodies. Failing to meet these obligations can lead to serious repercussions, including regulatory sanctions, legal proceedings, financial penalties, and reputational harm that can compromise the long-term viability of the operator.

Beyond compliance, strong AML/CFT protocols demonstrate a clear commitment to ethical conduct and responsible gaming. Such transparency fosters consumer confidence, reassuring players that the platform operates with integrity and in alignment with regulatory expectations.

Moreover, effective AML/CFT controls are crucial for mitigating internal risks associated with financial crime. Through detailed identity checks, systematic monitoring of transactions, and structured reporting of suspicious behaviour, gaming companies can minimize exposure to financial threats and regulatory breaches.

In essence, well-defined AML/CFT policies are fundamental to preserving the integrity of financial processes, maintaining legal compliance, enhancing consumer trust, and safeguarding against operational vulnerabilities in the gaming environment.

1.1 What is the meaning of AML/CFT?

Money Laundering (ML) refers to the process through which individuals or entities conceal the origins of illegally acquired funds, making them appear legitimate. This illicit activity poses a serious threat to the integrity of financial systems and is often linked to broader criminal enterprises. The laundering process generally unfolds across three key stages:

- **Placement** – Illicit proceeds are first introduced into the financial system, often through cash-heavy channels such as casinos, real estate, or other businesses with high volumes of cash transactions.
- **Layering** – A series of complex transactions—including fund transfers between accounts, currency conversions, international movements, and structured deposits—are employed to obscure the illicit origin of the funds.
- **Integration** – The ‘cleaned’ money is then reinvested into the formal economy through legitimate-looking ventures, such as property purchases, business investments, or luxury goods, making it extremely difficult to trace back to its criminal origin.

Although commonly associated with narcotics trafficking, money laundering also stems from crimes including human trafficking, fraud, corruption, arms smuggling, and large-scale tax evasion.

Terrorist Financing (TF) involves the collection or provision of financial resources to support terrorist individuals, groups, or activities. Unlike money laundering, TF often involves funds that originate from lawful sources—such as donations, personal income, or legitimate business revenue—but are ultimately used to fund unlawful terrorist acts. Methods of terrorist financing include the smuggling

of cash, use of prepaid debit cards, structured transactions, informal value transfer systems, and wire transfers, with the primary focus being to conceal the destination of the funds rather than the source.

Proliferation Financing (PF) concerns the provision of financial resources for the production, acquisition, or dissemination of weapons of mass destruction (WMDs), including nuclear, biological, and chemical weapons. This form of financing is globally condemned due to the severe threat it poses to international peace and security, and is governed by strict sanctions frameworks and export controls.

Targeted Financial Sanctions (TFS) are legally binding measures requiring financial institutions and businesses—such as casinos—to freeze and block the assets of individuals, organizations, or entities designated by the United Nations Security Council or the European Union. In Curaçao, adherence to these sanctions is legally mandated. Casinos are required to ensure that no funds, assets, or financial services are made available, directly or indirectly, to designated parties. They must also report any such occurrences to the Financial Intelligence Unit (FIU) and update their internal AML/CFT policies to reflect any changes to relevant sanctions lists.

At Green Forest Group, we are fully committed to enforcing stringent Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Proliferation Financing (PF) controls. In alignment with Curaçao's legal framework, our approach is proactive, risk-based, and regularly updated to identify, prevent, and report suspicious financial activities that could compromise the integrity of our operations or the global financial system.

2. Responsibilities

The Compliance Officer is responsible for the comprehensive oversight of all player transactions and for ensuring the accurate verification of the identities of all registered users. This role involves establishing clear criteria and monitoring systems to swiftly detect any potentially suspicious behaviour or irregularities in player activity. In addition to identification, the Compliance Officer is also tasked with designing, implementing, and continuously refining protocols aimed at addressing such anomalies effectively. These measures are intended to minimize exposure to financial crime and ensure that risks related to money laundering and the financing of terrorism are mitigated to the lowest reasonably achievable level, in line with regulatory expectations and the Company's risk appetite.

3. Company Policy and Procedures

3.1 Suitability

To access the gaming services provided by Green Forest Group N.V., players must first complete a full account registration through the brand's official platform. Participation in any gaming activities, including placing wagers, is restricted exclusively to individuals who have successfully registered an account. Only upon completion of the registration process and the explicit acceptance of the platform's Terms and Conditions and Privacy Policy, are players granted access to deposit funds and engage in gameplay.

As part of the account creation procedure, users are required to provide specific personal details that support both identification and verification measures in accordance with the company's compliance obligations. These required fields include:

- Full legal first and last name;

- A strong, secure password (entered twice for confirmation in line with the company's Information Security Policy);
- A valid email address;
- Date of birth;
- Country and place of residence;
- A mobile phone number, including the international dialing prefix associated with the selected country of residence.

The platform enforces strict age verification protocols, whereby players must be at least 18 years of age to register, with a higher minimum age requirement of 21 for individuals registering from Estonia, in accordance with local legal mandates. The registration system is configured to automatically reject applications submitted by individuals who do not meet the legal age requirement.

Additionally, access is denied to individuals residing in countries classified as restricted jurisdictions due to local prohibitions or severe regulatory constraints regarding online gambling.

To enhance risk management and compliance with Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) obligations, the Company also performs background screening during registration to identify potential Politically Exposed Persons (PEPs). In the event a registrant is identified as a PEP, the Risk Manager will conduct a case-specific assessment to determine the appropriateness of account approval based on predefined risk evaluation criteria.

3.2 Activation of Account

Prior a newly registered player is able to log in for the first time, an automated email containing an account activation link is sent to the email address provided during the registration process. This message serves solely to confirm the validity of the email and does not include any confidential or sensitive information, such as the player's username or password, thereby maintaining the integrity and security of the registration process.

To activate their account, the player must click on the link included in the activation email. Only after successful activation will the player be granted access to their account dashboard and permitted to initiate their first deposit. The system is designed to block any deposit attempts from accounts that remain unverified or inactive, ensuring compliance with identity verification requirements and enhancing the security of the platform from the outset.

3.3 Know Your Customer

In line with the regulatory requirements set forth by the National Ordinance on the Reporting of Unusual Transactions (NORUT) and the National Ordinance Identification for Services (NOIS), Green Forest Group N.V. places the highest priority on verifying the identity of its players. This process is fundamental for ensuring compliance with Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) obligations applicable in Curacao.

Accordingly, the Company requires all players to undergo identity verification when specific thresholds are met or certain risk indicators are triggered. Verification documents can be submitted either via the official customer support email listed on the Company's website or directly uploaded through the secure section of the player's registered account.

Acceptable identification documentation includes:

- A clear copy of a valid government-issued identification document (passport, ID card, or driver's license).
- Proof of address (e.g., a utility bill or official correspondence not older than three months).
- If applicable, a copy of the front and back of the payment card (with the middle eight digits and CVV/CVC code masked).
- Bank account statements or screenshots to confirm the origin of funds or ownership of the payment method used.

Implementation of Customer Due Diligence (CDD) is mandatory under the following circumstances:

- When a player engages in financial transactions totalling or exceeding NAf. 4,000 (approximately €2,000), whether in a single transaction or multiple linked transactions.
- When processing any occasional or one-time transaction that exceeds the above threshold.
- Whenever there are indicators or suspicions of money laundering or terrorist financing activity.
- If there is doubt about the validity, reliability, or adequacy of previously collected identification data.

Until a player's identity has been fully verified in accordance with these criteria, withdrawals will be strictly prohibited. Players are required to submit the requested verification documentation within a 30-day period from the date of request. Failure to do so may result in the temporary suspension or permanent deactivation of the account, in accordance with Curaçao's licensing standards and the Company's internal AML policies.

Withdrawal Policy and Payment Method Verification: Withdrawals must be processed using the same method that was used to fund the account, in order to prevent misuse or third-party transactions. If that method is unavailable, an alternative method previously used by the player or a secure bank transfer may be approved. In the case of bank transfers, staff are required to verify that the account belongs to the registered player. Cash withdrawals are strictly prohibited under Curacao's AML regime.

Ongoing Risk Assessment and Enhanced Due Diligence (EDD): As part of the Company's risk-based approach, all registered players are subject to ongoing risk assessment. Players identified as posing a higher risk—due to factors such as transactional behaviour, country of origin, or source of funds—will be required to undergo Enhanced Due Diligence. This includes, but is not limited to:

- Verification of ownership of all used payment instruments;
- Submission of documentary evidence confirming the source of funds or wealth;
- Additional scrutiny of account activity.

The Company ensures that all identity verification procedures and due diligence measures are implemented in a manner that is proportional to the risk presented, as mandated under Curaçao AML/CFT legislation.

3.4 Players' Risk Levels

Upon registration, each player is automatically assigned a risk classification within the system—Level 1 (Low Risk), Level 2 (Medium Risk), or Level 3 (High Risk)—based on preliminary KYC data and behavioral indicators.

- Level 1 – Low Risk: These players are granted full access to gaming services once standard KYC verification is completed. Their account activity is monitored in real time by automated systems designed to detect unusual patterns, such as sudden spikes in deposits or wagers. Any anomalies trigger alerts for further review.

- Level 2 – Medium Risk: In addition to standard monitoring, Medium Risk players are placed on a risk observation list reviewed weekly by management. Their withdrawal requests require prior approval from senior staff. Depending on the outcome of enhanced due diligence, they may be downgraded to Low Risk or escalated to High Risk based on emerging risk factors.
- Level 3 – High Risk: Players classified as High Risk are restricted from all site activity until a comprehensive enhanced due diligence review is completed. If a player's risk level is upgraded to Level 3 after a withdrawal is initiated, the transaction is immediately paused pending verification. These players are also notified of the elevated risk status and required to submit further documentation, including a real-time photo with their ID in cases of identity uncertainty.

Only designated personnel have the authority to adjust a player's risk level at any stage of the lifecycle.

3.5 Verification based on Risk

The depth of identification and verification procedures depends on the player's assigned risk level:

- Low Risk:

Basic verification is conducted by collecting and validating key personal details such as the player's full name, country and place of residence, and date of birth. This information is cross-checked to confirm identity before account functionality is enabled.

- Medium Risk:

Players assessed as Medium Risk must submit all information required for Low Risk verification, along with additional data including residential address, place of birth, and nationality. A valid government-issued photo ID (e.g., passport or driver's license) is required to support this information.

- High Risk:

For High Risk players, the verification process includes all steps outlined for Medium Risk profiles. However, additional scrutiny is applied. Depending on the nature of the risk, the Company may require further documentation or supporting evidence to fully validate identity and address any potential red flags.

Verification may be performed using official documents or credible third-party sources. If residential address information is not verifiable via submitted identification, the player must provide proof of address dated within the past six months. Acceptable documents include recent bank or utility statements, government-issued correspondence, or certified certificates of conduct.

To enhance verification reliability, Green Forest Group may also employ digital verification tools, including electronic IDs (e-ID), banking identity systems (Bank-ID), and reputable commercial databases. Daily monitoring processes—such as IP analysis and geolocation tracking—are conducted to detect inconsistencies.

Where standard methods fail to adequately confirm a player's identity or address, the Company escalates the case through Enhanced Due Diligence (EDD). This ensures a comprehensive and risk-sensitive verification approach is maintained in line with Curacao's regulatory expectations.

3.6 Medium and High Risk Customers

As part of its commitment to maintaining a secure and transparent remote gaming environment, Green Forest Group requires all players to open an account before accessing services. To further strengthen due diligence practices, the Company employs a customer risk profiling system, which is grounded in data-driven analysis. This system incorporates official economic and statistical indicators to construct behavioural benchmarks, enabling the evaluation of player activity against expected norms.

While routine transactions from customers not considered high risk do not warrant direct collection of Source of Wealth (SoW) information, this changes upon reaching Customer Due Diligence (CDD) thresholds. Once these thresholds are triggered, the approach to SoW varies based on the customer's risk classification:

- Medium Risk Customers

For customers categorized as Medium Risk, the Company uses statistical models derived from country-specific median income data to form a baseline understanding of typical wealth patterns. As these models offer reliable insight, formal SoW declarations are generally not required. However, where such declarations are voluntarily provided or requested for specific purposes, players must disclose the origin of their wealth (e.g., salaried employment, self-employment, business ownership). The declared information must be coherent with the customer's observed behaviour throughout their relationship with the Company.

- High Risk Customers

Individuals assessed as High Risk are subject to enhanced scrutiny. In these cases, the Company requires a full Source of Wealth declaration, accompanied by verifiable documentation. Additionally, if customer behaviour deviates from established norms—such as unusually large or frequent deposits—the Company may also request Source of Funds (SoF) information. This includes specific details about the expected origin, value, and frequency of incoming funds.

In all instances, the Company does not accept SoW or SoF declarations at face value. Claims must be corroborated with supporting evidence. For example, a customer citing employment as the origin of their wealth may be asked to provide recent bank statements, pay slips, or employment contracts as proof.

This structured approach ensures that customer profiles remain accurate, risk-sensitive, and compliant with Curaçao's AML/CFT regulatory framework.

4. AML Procedures

All financial interactions between players and Green Forest Group must be conducted solely through the payment methods explicitly offered by the Company. These options may be updated at the Company's discretion. Under no circumstances are peer-to-peer (player-to-player) transfers allowed on the platform.

To uphold strict compliance with Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) regulations, every transaction is subject to systematic monitoring and risk-based analysis. This ensures the timely identification of patterns or activities indicative of money laundering or the financing of terrorism.

If credible information suggests that a player may be engaged in financial misconduct or illicit transactions, the Company will escalate the matter to the Financial Intelligence Unit (FIU) Curaçao without delay. All suspicious activities are first reported to the Money Laundering Reporting Officer (MLRO) using the Suspicious Transaction Report (STR) framework. The MLRO will assess the situation and, if warranted, formally submit the case to the FIU.

The MLRO is responsible for ensuring that the Company maintains and enforces effective AML/CFT systems in line with legal obligations and industry best practices. In the temporary absence of the MLRO—such as during leave—the Company Director will assume these responsibilities to maintain uninterrupted compliance oversight.

All transaction procedures, including AML-specific provisions, are detailed in the Company's Terms and Conditions. Any amendments to these policies are clearly communicated to all registered players in writing before such changes are implemented.

4.1 Training Related to AML

In partnership with the Money Laundering Reporting Officer (MLRO) and any necessary external parties, comprehensive training sessions covering our Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) policies and procedures will be provided to all new hires and key collaborators.

New employees must complete this training within their first month of employment, followed by a quiz or test to assess their understanding. Upon successful completion, their participation will be confirmed by their direct manager, with proof securely stored in their employee file.

Moreover, all employees will review the training materials ahead of their annual performance evaluations. During these reviews, any relevant updates or changes to the policies and procedures will be communicated.

The training will ensure that employees fully understand the following key areas:

- Legal obligations regarding money laundering and the financing of terrorism.
- Their personal responsibilities under applicable regulations.
- Internal reporting procedures for relevant issues.
- The company's measures to prevent money laundering and terrorist financing.
- Protocols for identification, verification, record-keeping, and other preventative actions.
- Procedures for detecting and managing suspicious transactions.
- The potential personal liability for failure to report relevant information or suspicions, as required by regulations and internal policies.
- Current trends, techniques, and methodologies in the field of money laundering and terrorist financing.

4.2 Calculation of Risk

Green Forest Group adopts a risk-based approach to Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT), focusing on key risk indicators to ensure robust compliance. These practices align with AML best practices to prevent and detect financial crime:

- FATF-Identified High-Risk Countries: Countries flagged by the Financial Action Task Force (FATF) due to insufficient AML/CFT controls are subject to heightened scrutiny. Players attempting to register from these jurisdictions are either blocked from registering or automatically categorized as high-risk.

- Internally-Identified High-Risk Countries: Based on the company's own risk assessment, certain countries deemed to pose an elevated AML/CFT risk will automatically classify players from these regions as high-risk.
- Large Transactions Within a 30-Day Rolling Window: Transactions that exceed a significant threshold over a 30-day rolling period will trigger additional monitoring. Deposits are temporarily frozen, and enhanced due diligence (EDD) is required before funds can be released.
- Risky Payment Methods: Players utilizing high-risk payment methods, such as prepaid credit or debit cards, will be reclassified as high-risk to mitigate potential AML/CFT concerns.
- Quarterly Risk Reviews by the MLRO: The Money Laundering Reporting Officer (MLRO) conducts quarterly risk assessments to identify new and emerging risks. Any identified risks are promptly integrated into the Customer Due Diligence (CDD) framework, with relevant updates communicated to all staff members.
- Monitoring of AML/CFT Warning Lists: The company maintains and regularly updates a list of individuals and entities flagged in AML/CFT-related warning lists, ensuring enhanced monitoring and oversight of these subjects.
- Verification of Source of Funds: The company ensures thorough verification of the source of funds, particularly for players undergoing enhanced due diligence (EDD), to prevent illicit financial activity.

By incorporating these risk-based measures, the company maintains a comprehensive AML/CFT framework that proactively identifies and mitigates risks associated with money laundering and terrorist financing.

4.3 PEPs – Politically Exposed Persons

In line with our commitment to stringent Anti-Money Laundering (AML) compliance, Green Forest Group N.V. enforces enhanced due diligence (EDD) procedures for foreign Politically Exposed Persons (PEPs), whether as customers or beneficial owners. These procedures include:

- Risk Management Systems: Robust systems are in place to identify whether a customer qualifies as a PEP, ensuring effective risk management from the outset.
- Senior Management Approval: Before establishing or continuing a business relationship, approval must be obtained from senior management or the Compliance department. This applies to both new and existing customers, as well as occasional transactions.
- Verification of Source of Wealth and Funds: We take reasonable steps to verify the origin of a PEP's wealth and funds. This includes requesting a declaration from the customer and cross-checking information with reliable, independent sources. In cases where public sources are insufficient, additional documentation may be requested.
- Enhanced Ongoing Monitoring: We continuously monitor business relationships on a risk-based approach to detect any suspicious activity, ensuring that all potential risks are identified and addressed promptly.

Furthermore, we ensure that domestic PEPs and individuals holding prominent roles within international organizations are also identified, and if higher risks are detected, the enhanced due diligence measures will be applied accordingly.

While all PEPs undergo stricter due diligence, a risk assessment is conducted on an individual basis to tailor the necessary controls. These measures also extend to the family members and close associates of PEPs.

Screening for PEP status is conducted during the customer onboarding process and continues throughout the business relationship. If a customer who was not initially identified as a PEP

subsequently attains PEP status, enhanced due diligence will be implemented within 30 days. Failure to comply with these requirements will result in the immediate termination of the business relationship.

4.4 Risk Monitoring

All user activities are comprehensively documented and monitored, with high-risk actions subject to heightened and frequent scrutiny. Senior management holds weekly meetings to review reports on these high-risk activities, ensuring a thorough evaluation. This manual review process operates alongside an automated flagging system designed to identify potential irregularities, which is safeguarded by robust security controls. These controls allow for the implementation of exposure limits on players, promoting effective risk management.

The system specifically monitors the following high-risk areas:

- Large Transactions: Transactions exceeding NAF 4,000 (EUR 2,000) or showing similar high deposit patterns, or those deemed significant by the Company.
- High-Risk Jurisdictions: Users originating from jurisdictions with high-risk profiles, as identified by the Financial Action Task Force (FATF).
- High-Risk Payment Methods: Deposits made through payment channels that are classified as high-risk.
- Politically Exposed Persons (PEPs) and Sanctioned Individuals: Ongoing monitoring of PEPs and individuals listed on sanctions lists.
- Deviations in User Activity: Identification of deposit or wagering behaviours that significantly differ from a player's historical patterns.
- Suspicious Player Strategies: Scrutiny of unreasonable or suspicious player strategies that may indicate potential fraud or high risk.

These measures ensure a proactive approach to identifying and mitigating risks associated with money laundering and other illicit activities.

4.5 Monitoring of Transactions – Customer Risk

To ensure comprehensive oversight of transactions within the Company's operations and strengthen the monitoring protocols outlined earlier, individuals will be classified into risk categories based on their behaviour and related data.

Low Risk

Individuals will be classified as low-risk if they meet the following criteria and have not previously been assigned to another risk category:

- Transactions or deposits do not exceed €2,000.
- No alerts or suspicions are triggered by their activity.

Customers identified as low-risk will undergo standard Customer Due Diligence (CDD) procedures and must provide a valid identification document (such as a national ID or passport) for identity verification through reputable, independent sources.

Medium Risk

Individuals who meet certain criteria, which may include suspicious transaction patterns or inconsistencies, will be classified as medium risk. These individuals are characterized by:

- Deposits, payment methods, and transaction timelines contributing to their medium-risk classification.
- Alerts or flagged transactions, particularly those involving inconsistencies in geolocation or payment methods.

An automated alert is triggered when a customer exceeds €5,000 in deposits within a 30-day period. Agents may manually escalate the customer's risk level to high if additional alerts or inconsistencies are detected.

Medium-risk customers will undergo Enhanced Due Diligence (EDD) verification and continuous monitoring to ensure compliance with regulations and mitigate potential risks effectively.

High Risk

High-risk customers are identified by the following characteristics:

- Large deposit amounts, unusual payment methods, and/or irregular transaction timing.
- Association with Politically Exposed Persons (PEPs).
- Residency or citizenship in high-risk countries.
- Current suspicions related to money laundering or other illicit activities.

An automated high-risk alert is triggered when a customer exceeds €10,000 in deposits within a 30-day period or as defined by the Company.

High-risk customers will undergo thorough Enhanced Due Diligence (EDD) procedures, including continuous monitoring, to ensure full regulatory compliance and effectively mitigate identified risks.

4.6 Business Relation Obligation

The record-keeping procedures outline the types of Anti-Money Laundering (AML) data to be retained and specify the minimum retention period in compliance with the Company's Implementing Procedures. These protocols distinguish between different data sets based on risk categorizations, as detailed in additional procedures, and address the proper storage of AML-related documents on secure technical infrastructure, ensuring compliance with privacy laws.

Identification Records

Documentation collected for risk categorization includes:

- Player personal details from registration or later stages.
- Results of automated identity verification.
- Copies of identification documents and proof of address.
- Additional documents required based on the player's risk category, such as source of wealth verification.

Employee records include personal information, CVs, certificates of good conduct, and records of completed AML/CFT training.

Transaction Records

All transaction data should be digitally archived on the Company's infrastructure and include:

- Methods used for deposits and withdrawals.
- Source and destination of funds.
- Credit card transaction approvals.

- Transaction volumes.

AML Legislation Records

Required documentation for compliance with PMLFTR includes:

- Internal reports submitted to the Money Laundering Reporting Officer (MLRO).
- MLRO determinations, including explanations for not filing Suspicious Transaction Reports (STR) with the FIU Curacao.
- STRs submitted to the FIU and follow-up reports.
- MLRO reports to senior management, including assessments of Politically Exposed Persons (PEPs).
- Senior management's written deliberations on MLRO recommendations.
- Internal AML audits and training verification documents.

These procedures ensure the secure and compliant storage of AML data while protecting personal privacy.

4.7 Reporting of Transactions

In line with its internal procedures, the Company is obligated to adhere to the National Ordinance for Identification of Services and comply with the legal requirements for detecting and reporting unusual transactions, whether these transactions are completed or attempted. The casino must implement comprehensive procedures that address the following critical areas:

- Identification of Unusual Transactions: Establishing effective methods and systems to detect transactions that deviate from regular patterns or those that raise suspicion due to their nature, volume, frequency, or any other red flags.
- Documentation of Unusual Transactions: Maintaining thorough and accurate records of any transactions deemed unusual. These records must be detailed and readily available for review and submission to authorities as necessary.
- Reporting of Unusual Transactions: Ensuring that any identified unusual transactions are reported promptly and in compliance with applicable laws and regulations. This includes submitting the required reports to relevant authorities, such as the Financial Intelligence Unit (FIU), and following up with any required actions or documentation.

These procedures are designed to ensure that all potentially suspicious transactions are identified, documented, and reported in a timely manner, thus ensuring compliance with legal and regulatory obligations.

4.1.1 Identification of Unusual Transactions

At Green Forest Group, recognising unusual transactions requires a comprehensive understanding of each player's profile and behaviour. The purpose of gathering detailed player information is to assess associated risks and create a customer profile that helps predict their actions within the business relationship.

In compliance with NORUT legislation, we have implemented both objective and subjective indicators to help management guide staff in identifying and appropriately documenting unusual transactions. All identified unusual transactions must be reported to the Compliance Officer using the format approved by management. Along with the transaction details, supporting documents such as identification copies, cash-out slips, and any other relevant materials must be submitted. The Compliance Officer is responsible for ensuring these records are properly filed and maintained.

If any internally flagged transactions are not submitted to the Financial Intelligence Unit (FIU), the reasons for this must be thoroughly documented and signed off by the Compliance Officer and/or management. This ensures transparency and accountability in the decision-making process.

To align with FATF Recommendation 11, special attention will be given to complex, unusually large transactions or patterns that lack a clear lawful or economic purpose.

What is Considered an Unusual Transaction?

- Transactions linked to money laundering or terrorism financing that are reported to law enforcement or the Department of Justice.
- Transactions involving entities or individuals listed under the Sanctions National Ordinance (N.G. 2014 no. 55).
- Transactions of NAf. 5,000 or more, regardless of whether the payment is made electronically or via other non-physical methods. This includes, but is not limited to:
 - Cashless transactions exceeding NAf. 5,000, such as transfers from the casino's bank account to a local or international bank account at the client's request.
 - Accepting or releasing deposits of NAf. 5,000 or more at the client's request.
 - Sale of chips (or tokens/credits) for NAf. 5,000 or more to a customer.
 - Cashing out NAf. 5,000 or more.

A transaction may be considered unusual as a one-time occurrence or a series of transactions totalling NAf. 5,000 or more within a single gaming day.

- Presumed Money Laundering or Terrorist Financing Transactions: Transactions that raise suspicions of being linked to money laundering or terrorist financing activities.

By following these guidelines, Green Forest Group ensures that all unusual transactions are properly identified, documented, and reported in line with AML best practices.

4.1.2 Documentation of Unusual Transactions

We will register with the Financial Intelligence Unit (FIU) and obtain access to the goAML reporting portal once the FIU validates our registration. The goAML portal allows for bulk reporting, and the casino's account manager at the FIU should be contacted to confirm eligibility for this service.

The Compliance Officer is responsible for preparing and submitting reports of all unusual transactions to the FIU in compliance with their reporting regulations. These reports, along with any supporting documents, must be submitted in English via the goAML portal.

The casino, including its directors, officers, and employees, is legally protected from criminal and civil liability for any breach of confidentiality when providing information to the FIU in accordance with the reporting requirements.

4.1.3 Reporting of Unusual Transactions

In compliance with Article 11 of the NORUT, any unusual transactions or attempts to carry out unusual transactions must be reported to the Financial Intelligence Unit (FIU) without delay. We have established clear procedures for both internal and external reporting of such transactions, ensuring that these protocols are communicated to all relevant personnel.

Any unusual transactions, whether individual or part of a series, as specified in the Regulation Indicators for Unusual Transactions, must be immediately reported internally. Each report will be accompanied by the necessary supporting documentation.

4.8 Record Keeping

In full alignment with the National Ordinance on the Identification of Services (NOIS), the National Ordinance Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (N.G. 2014, no. 55), and the Kingdom Sanctions Act (N.G. 2016, no. 54), the Company maintains robust record-keeping procedures that ensure the secure collection, classification, and retention of data essential for Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) compliance.

The following categories of documentation must be preserved:

- Evidence of the application of a risk-based approach, including the Business Risk Assessment (BRA), alongside relevant policies and procedural manuals.
- All Customer Due Diligence (CDD) materials, in accordance with Section 9.2(b) of Part 1 of the Implementing Procedures.
- Full records of established business relationships and associated transactions, as specified in Section 9.2(c) of Part 1 of the Implementing Procedures.
- Internal reports submitted to the Money Laundering Reporting Officer (MLRO), including documented reasoning for any decisions not to file a Suspicious Transaction Report (STR) with the FIU.
- Copies of all STRs submitted to the FIU and any additional follow-up documentation.
- Verified documentation of AML/CFT training completed by employees.
- Employee vetting records, such as conduct certificates and screening-related documentation.
- Agreements and documentation regarding any outsourced compliance or operational functions.

All of the above data will be stored securely on the Company's servers and retained for a minimum of five (5) years from the date of the customer's last recorded transaction, marking the cessation of their active relationship with the Company.

In addition, detailed records of all AML/CFT-related reports and regulatory inquiries will be kept. These records will capture the date, nature of the inquiry, identity and authority of the requesting body, legal basis for the request, individuals or accounts involved, and any associated transactions.

Our record management framework is strictly guided by data protection laws and privacy regulations. Ongoing reviews and updates will be carried out to ensure full legal compliance with any evolving statutory requirements.

5. Employee Screening and Training

We are dedicated to upholding the highest standards of integrity and ensuring full adherence to all applicable legal and regulatory requirements governing financial transactions. To support this commitment, the Company will establish and rigorously apply comprehensive internal policies and controls, including mandatory background checks to assess prospective employees for any criminal history.

Furthermore, we will design and implement specialized training programs for all personnel engaged in activities that involve the handling or monitoring of transactions, particularly those that may be identified as unusual under the Ministerial Decree on Indicators for Unusual Transactions (N.G. 2015 no. 73). These programs will provide clear expectations for professional conduct and reinforce the principles of Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) compliance.

Training initiatives will be role-specific, ensuring that employees receive relevant and practical knowledge tailored to their departmental functions. As a baseline, all AML/CFT training will cover the following core components:

- Legal and regulatory obligations relating to AML/CFT;
- Identification and reporting of unusual or suspicious activity;
- Use of internal reporting channels and escalation protocols;
- Data protection and confidentiality requirements; and
- Consequences of non-compliance for both the employee and the organization.

These sessions will be conducted regularly and updated in response to legislative changes or emerging risks to ensure that staff maintain a high level of awareness and capability in managing AML/CFT responsibilities.

5.1 New Joiners

All newly hired staff members who engage directly with customers or are involved in processing customer transactions—regardless of their role or seniority—must undergo in-depth training focused on anti-money laundering (AML), counter-terrorist financing (CTF), and the mandatory reporting of unusual activities to the designated compliance officer.

This initial training will provide a clear understanding of the legal and regulatory landscape surrounding money laundering, terrorist financing, and proliferation financing. It will familiarize employees with the organization's internal AML/CTF framework, including operational policies, procedural controls, and statutory reporting obligations.

Training will also address industry-specific risks by examining money laundering methods and emerging trends relevant to the gambling sector. A significant emphasis will be placed on effective customer due diligence (CDD) processes and how to assess risk profiles. Staff will be taught to identify and respond to both objective and subjective red flags associated with suspicious transactions, ensuring they are fully equipped to act in line with the company's compliance expectations from day one.

5.2 AML Compliance Team

Personnel responsible for overseeing the Anti-Money Laundering (AML) program must receive advanced, role-specific training to ensure they remain up to date with the evolving landscape of financial crime and the corresponding regulatory developments. This specialized training is critical for enhancing the organization's ability to effectively identify, assess, and mitigate emerging AML/CTF risks.

In addition to ongoing internal knowledge development, AML officers and designated compliance staff are encouraged to participate in external professional development opportunities. These may include attending accredited seminars, industry conferences, regulatory briefings, and specialized workshops led by recognized experts in AML, counter-terrorist financing, and sanctions compliance. Such engagements provide a valuable forum for gaining deeper insights into current typologies, enforcement priorities, technological advancements (such as AI-driven monitoring tools), and international best practices.

The training will also equip AML program leaders with the skills necessary to update internal policies, strengthen oversight mechanisms, and provide effective guidance to other departments. This proactive approach ensures the organization's AML framework remains robust, compliant, and responsive to both local and global threats.

5.3 Management

Senior Management, including both departmental Managers and members of the Board of Directors, must undergo advanced training covering all critical aspects of money laundering, terrorist financing, and the applicable internal policies, procedures, and regulatory obligations. This training is essential to ensure that leadership is equipped with the knowledge needed to oversee and support a compliant and effective AML/CFT framework.

Furthermore, ongoing communication regarding money laundering risks and emerging threats must be maintained at the executive level. Regular updates and risk assessments should be presented to the Board to keep them informed of any developments that may impact the organization's integrity and reputation. This ensures that strategic decisions are made with a clear understanding of the potential legal, financial, and reputational consequences related to financial crime exposure.

5.4 Training Program

Ongoing refresher training must be conducted at regular intervals to ensure that employees remain well-informed about emerging risks, evolving money laundering and terrorist financing techniques, and any changes to regulatory expectations. This continuous learning approach helps staff maintain the necessary competence to identify and respond to suspicious activity effectively.

To verify compliance with these training obligations, the casino is required to keep detailed records of all training activities. These records should include the full content of the training sessions, a list of participants, training dates, results of any knowledge assessments or evaluations conducted, and a structured plan outlining future training initiatives. This documentation supports regulatory transparency and reinforces the company's commitment to sustained AML/CFT awareness and performance.

6. Consequences of non-Compliance

Failure to comply with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) obligations may result in serious legal, regulatory, financial, and reputational consequences for both the Company and its employees. These consequences are not limited to deliberate breaches but also extend to failures resulting from negligence, oversight, or inadequate internal controls.

- Regulatory Sanctions: Non-compliance may lead to enforcement actions by the Financial Intelligence Unit (FIU) or other regulatory authorities. This can include:
 - Administrative fines and penalties.
 - Suspension or revocation of the Company's operating license.
 - Mandatory audits or corrective measures imposed by regulators.
- Criminal and Civil Liability: Both the Company and individual employees which including directors, officers, and agents may face criminal prosecution or civil litigation in cases involving:
 - Wilful neglect or concealment of suspicious activities.
 - Failure to report unusual or suspicious transactions.
 - Knowingly facilitating money laundering or terrorist financing.
- Employment Consequences: Employees found to be non-compliant with AML obligations, whether through intentional misconduct or failure to follow established procedures, may be subject to disciplinary action. This may include:
 - Formal warnings.
 - Suspension.
 - Termination of employment.

- Referral to law enforcement or regulatory bodies if criminal activity is suspected.

7. Payout Management

Green Forest Group will only accept and process payments through accounts maintained with licensed financial institutions or authorized payment service providers (PSPs) that are fully approved and not restricted by the relevant Authority. Engagements with any PSPs will commence strictly after the official reactivation of the Company's license has been granted by the Authority.

All player deposits and licensee-held funds will be accurately credited to the respective player accounts, ensuring complete traceability and separation of funds. The Company will not permit or facilitate any transactions involving cash deposits or cash withdrawals directly between players and the Company under any circumstances, thereby reinforcing transparency and AML/CFT safeguards.

To manage dormant player balances, the Company may establish an inactive account policy. This procedure will be designed to identify accounts that have remained unused over a defined period. Dormant players may be subject to a monthly inactivity fee, which will only be applied following a minimum 30-day advance notice to the account holder.

The implementation and structure of this process will be determined by senior management, in line with player protection standards as outlined in the Authority's Player Protection Directive and any other applicable legislation. The inactive account procedure will be monitored regularly to ensure it remains fair, transparent, and compliant with regulatory expectations.

7.1 Deposit Process

Green Forest Group follows a structured deposit process to ensure security and transparency. Players must first register through the app and complete all required Know Your Customer (KYC) checks to verify their identity. Once registered, they access the Deposits page, where a variety of popular, country-specific deposit methods are offered, typically including credit cards, debit cards, and eWallets approved by the Financial Services Authority (FSA).

After selecting a deposit method and amount, players are redirected to a certified Payment Service Provider (PSP) for processing. Upon transaction submission, the Company awaits confirmation from the card acquirer or eWallet provider. Once approved, the transaction details are recorded in the player's account and stored in the database for accuracy and future access.

The Company employs strict fund protection measures, ensuring all player balances are fully backed by designated bank accounts and PSP wallets. At least 90% of player funds must be held in segregated accounts as per regulatory obligations, guaranteeing player balances are always covered.

To strengthen oversight, the Board regularly reviews reports on the segregation of player funds versus system-recorded balances. Daily reconciliations are conducted between Protected Player Fund accounts and system balances, and if discrepancies are found, additional funds are promptly transferred to maintain full compliance and player confidence.

7.2 Withdrawal Process

To withdraw funds, players must select an approved payout method through the Accounts page on the website. The available balance eligible for withdrawal is displayed, and players choose the withdrawal amount and method. Withdrawals must be returned via the same deposit method (e.g., credit card or eWallet) used for the original deposit, where applicable.

The Company then conducts a thorough verification process, including checking KYC documentation, validating identity, reviewing for duplicate accounts, and requesting additional documentation if needed. Once the withdrawal is approved, it is forwarded to the Payment Service Provider (PSP) for processing. The PSP confirms the transaction outcome, and the player's balance is updated accordingly.

The website is then updated to reflect the player's revised account balance in real-time.

7.3 Handling of Funds

All valid wagers must be made using funds securely held in a player's wallet, ensuring funds are available via successful transfers or confirmation from the card issuer or original funding source. These funds can be used for wagers or withdrawn back to their original account, but cannot be transferred between user accounts.

Players have access to detailed records of all fund movements, including inbound and outbound transactions and funds used for wagers. These details are visible in the player's wagering summary and wallet page, showing the balance before and after each transaction.

Wager outcome regulations, including those for non-winning wagers, are transparently displayed on the site. The system is designed to prevent loss of data or funds during service interruptions, although temporary issues may prevent placing wagers. The platform is built with High Availability (HA) to minimize the impact of such disruptions.

8. Contact Information

For any questions regarding this policy please contact:

Licensee Name: Green forest Group N.V.

Address: Zuikertuintjeweg Z/N (Zuikertuin Tower)

Phone Number: +35679052363

Email Address: compliance@epybet.com