

Green Forest Group N.V.
Customer Risk Assessment
(CRA)

Table of Contents

1.	Overview and Objective	3
2.	Process and Approach.....	3
3.	Risk Scoring	4
3.1	Customer Risk.....	4
3.2	Product and Transaction Risk.....	5
3.3	Delivery Channel Risk	6
3.4	Geographical Risk	6
4.	Process for Due Diligence	7
4.1	Enhanced Due Diligence	8
5.	Sanctions.....	9

1. Overview and Objective

Green Forest Group N.V (referred to as "the Company") has established procedures to assess the risk associated with each customer who registers to use its gaming services.

The Company conducts a manual risk evaluation as part of the Customer Due Diligence (CDD) process whenever a customer's activity reaches a threshold of NAF 4,000 (approximately €2,000.00) in a single deposit or over a rolling period. This evaluation is carried out in accordance with the Financial Intelligence Unit (FIU) Guidelines, which identify four key risk factors:

- Customer Risk
- Product, Service, and Transaction Risk
- Distribution Channels Risk
- Geographical Risk

By analysing these factors, the Company seeks to thoroughly assess the potential risk presented by each customer. This enables the Company to make informed decisions and apply appropriate risk mitigation measures, ensuring compliance with regulatory requirements.

2. Process and Approach

The Company conducts a detailed manual customer risk assessment based on the information collected during the customer registration process. This assessment is initiated once a customer reaches the deposit threshold of NAF 4,000 (approximately €2,000.00). At this stage, a risk rating is assigned to the customer, categorizing them as low, medium, or high risk.

Depending on the assigned risk level, the Company applies different levels of due diligence:

- Low-Risk Customers: Standard Customer Due Diligence (CDD) procedures are followed, which include verifying basic customer information.
- Medium-Risk Customers: In addition to the standard CDD, the Company collects further details such as occupation, source of funding and wealth, place of birth, and nationality.
- High-Risk Customers: Enhanced Due Diligence (EDD) procedures are required, involving a thorough verification of all relevant documentation and a more extensive review of the customer's background.

This risk assessment determines the depth and frequency of the CDD process and ongoing monitoring required for each customer. It takes into account factors such as the customer's economic activities and/or sources of wealth (SOW).

The Customer Risk Assessment (CRA) is carried out within 30 days after the customer reaches the deposit threshold of NAF 4,000 (€2,000) within a rolling 180-day period. The outcome is a Customer Risk Profile, which is reviewed continuously throughout the course of the business relationship, especially as new information becomes available.

The customer relationship is considered to begin when the customer opens an online account through the Company's website. Moreover, the Company reserves the right to reassess the customer's risk level at any point during the business relationship, particularly if there are significant changes in the customer's behavior or financial activity. The customer's risk profile is reviewed at least semi-annually, or more often if certain trigger events occur, such as a substantial increase in spending or reluctance to provide the necessary documentation for CDD.

If the customer fails to provide the required documentation within 30 days of the request, the Company may suspend or even close the account, as stipulated by its internal procedures and regulatory obligations.

3. Risk Scoring

The Company defines the allocation of risk percentages across various categories as part of its comprehensive, risk-based approach. These allocations reflect the relative importance of each risk area in determining the overall risk associated with a customer. The risk categories and their corresponding allocations are as follows:

- **Customer Risk (30%):** This category evaluates the individual characteristics of the customer, including their financial background, occupation, and potential exposure to high-risk activities. A higher weight is assigned to customers whose profiles present elevated concerns regarding illicit activities or financial crime.
- **Product, Transaction, and Service Risk (40%):** This category focuses on the risk associated with the products, services, and transactions that the customer engages with. Higher percentages are allocated to high-risk products or services, such as those involving large or complex financial transactions, or gambling activities, which may present increased money laundering risks.
- **Delivery Channel Risk (10%):** This assesses the risk posed by the method through which services are delivered, including online channels or physical locations. Digital platforms or other remote services may carry higher risks due to their susceptibility to anonymous transactions or lack of face-to-face interaction.
- **Geographical Risk (20%):** This category evaluates the risk related to the customer's location and the jurisdictions they are connected to. Regions known for weak anti-money laundering controls or high levels of corruption may contribute to a higher risk assessment.

If a customer is identified as a Politically Exposed Person (PEP), their risk score is automatically increased to 100%, categorizing them as high risk. This is due to the increased potential for exposure to corruption or illicit financial activity often associated with such individuals. In line with the Company's Anti-Money Laundering (AML) Fraud Management policy, the Company reserves the discretion to either accept or decline the registration of PEPs based on an in-depth evaluation of the associated risks.

Both the business risk assessment and the customer-specific risk assessment focus on the same four core risk areas outlined above. These areas form the foundation for determining the appropriate level of due diligence required for each customer and are central to the Company's efforts to ensure compliance with AML regulations and mitigate the risk of financial crime.

3.1 Customer Risk

For the Company, a customer refers to a natural person who is either seeking to initiate or has already established a business relationship with the organization. The level of risk associated with each customer can vary significantly based on their individual profile. The Company exclusively engages with natural persons as customers, and the primary focus of the risk assessment process is their economic activities and/or sources of wealth.

The risk assessment process involves evaluating the consistency, reliability, and completeness of the information available about the customer. Verification of client identification is carried out using methods outlined in the Company's Anti-Money Laundering (AML) procedures, which are also applied during the initial assessment of the customer's risk profile.

Through this process, the Company identifies specific categories of clients or business relationships that present elevated risks. These clients are subject to increased monitoring and additional precautionary measures. Transactions involving individuals from jurisdictions that do not fully comply with international AML standards are given particular scrutiny.

In cases where transactions appear to lack reasonable economic justification or seem to lack a legitimate purpose, the Company proactively gathers supplementary information regarding the nature and objectives of the transaction.

Clients who currently or have previously held senior state positions, as well as those closely associated with them, are subject to a significantly higher level of scrutiny.

The risk assessment of a natural person is primarily based on their economic activities and/or sources of wealth. A customer with a steady, singular source of income is considered to present a lower risk for money laundering (ML) or terrorist financing (TF) compared to those with multiple or irregular income streams. This is due to the added complexities involved in verifying multiple income sources and ensuring that the amounts deposited and wagered align with the customer's declared sources of income during ongoing monitoring.

Heightened due diligence measures may include requesting additional documentation, conducting online research, obtaining references from counterparties, verifying income sources with employers, following directives from the Financial Intelligence Directorate, or implementing other appropriate measures as needed.

Certain business or professional activities from which a customer or beneficial owner derives wealth or funds carry a higher risk of ML and TF. These include activities involving large cash transactions, industries susceptible to corruption or financial crime (such as the firearms trade, defense sector, and mining industry), virtual currencies, and charitable organizations that facilitate fund transfers to high-risk jurisdictions.

On the other hand, activities deemed to present a lower risk of ML and TF include entities listed on regulated markets subject to strict disclosure requirements, businesses operating under effective financial supervision, and entities within the public administration.

Beyond business activities, other risk factors include individuals seeking residence rights or citizenship through capital investments, or individuals associated with Politically Exposed Persons (PEPs) or those holding prominent public positions that may be susceptible to misuse for personal gain.

3.2 Product and Transaction Risk

Certain products, services, and transactions naturally present higher risks and are more susceptible to exploitation by criminals. These include activities that allow customers to influence game outcomes, particularly through coordinated efforts. High-risk factors also involve specific funding methods like cash or anonymous payment options, such as prepaid cards or virtual currencies, which obscure audit trails and provide anonymity.

An especially high-risk factor involves the use of accounts or cards under third-party names to mask the true identity of the account holder. On the other hand, when customers transfer funds from bank accounts or cards registered in their name with reputable institutions in compliant jurisdictions, the risk of Money Laundering (ML) is lower.

The level of risk associated with a product, service, or transaction is influenced by factors like transparency, complexity, and value. Products or services that offer anonymity, such as nominee

accounts, are considered higher risk. Transactions that are complex, particularly those crossing international borders with multiple entities and jurisdictions, increase the level of risk. Additionally, products or services that involve cash transactions are seen as riskier compared to those with clear and traceable funding sources.

In summary, inherent risks are tied to the nature of the product, service, or transaction, particularly when factors like transparency, complexity, and cash usage are involved. Activities that enable high-value transactions or offer payment instruments with no limits or caps represent a higher risk compared to those with established restrictions. These limits should also be considered when assessing the level of risk.

3.3 Delivery Channel Risk

The Company's risk exposure in its business relationships and transactions is heavily influenced by the channels used for customer interaction and transaction execution. Channels offering anonymity inherently increase the risk of Money Laundering and Terrorism Financing (ML/TF) unless effective safeguards are in place. To counteract risks like identity fraud or impersonation, the Company applies technological solutions and additional risk-based measures.

Electronic databases help confirm that identification details match real individuals but are insufficient alone to verify true customer identity, requiring further verification steps. The risk also rises when third parties are involved, especially if they are not subject to AML/CFT obligations. Introducers like affiliates generally present a lower risk compared to third-party-operated physical establishments, where oversight of deposited funds is more challenging.

Overall, the risk level depends on how products and services are delivered. While non-face-to-face interactions are not automatically high risk, without proper technological controls, such scenarios can significantly elevate ML/TF risks. The Company carefully evaluates intermediaries' reliability and compliance standards when customers are introduced through third parties or internal networks.

3.4 Geographical Risk

The Company actively monitors and reviews reports and updates from authoritative sources such as the FATF (Financial Action Task Force) sanction lists, United Nations sanctions lists, and other country-specific evaluations to maintain an up-to-date understanding of geographical risk factors. Continuous awareness of these resources ensures that country risk assessments remain aligned with the latest global standards and threats.

In evaluating geographical risk, the Company considers several customer attributes, including nationality, country of residence, and place of birth. These factors are carefully analyzed, as they may indicate a heightened exposure to Money Laundering (ML) or Financing of Terrorism (FT) risks.

Customers who are linked to countries with known deficiencies in AML/CFT frameworks, countries listed on international sanctions lists, jurisdictions associated with high levels of corruption, or those sanctioned for terrorism financing or arms proliferation, are automatically classified as high-risk. On the other hand, customers associated with jurisdictions identified as having low or moderate ML/FT risk are categorized accordingly, subject to standard or simplified due diligence measures.

To determine geographical risk more comprehensively, the Company assesses multiple criteria, including:

- Jurisdictions identified by FATF, MONEYVAL, the International Monetary Fund (IMF), or other reputable sources as having serious shortcomings in their AML/CFT systems.

- Countries subject to international sanctions or restrictive measures by the UN, EU, or similar bodies.
- Nations known to support terrorist activities or organizations directly or indirectly.
- Countries exhibiting high levels of public sector corruption or weak governance standards.
- Jurisdictions lacking transparency regarding beneficial ownership, failing to meet international tax cooperation standards, or offering secrecy that can obscure the origin and ownership of funds.

This detailed analysis allows the Company to tailor its due diligence processes to the specific risks associated with each customer's geographical connections, applying enhanced measures where necessary to mitigate exposure to ML/FT threats.

4. Process for Due Diligence

Upon receipt of a customer's first deposit — which formally establishes a business relationship — the Company promptly initiates its Customer Due Diligence (CDD) procedures. This process begins even before the deposit is accepted, with an initial verification of the customer's identity and a cross-check to confirm there are no duplicate accounts registered under the same name, effectively minimizing the risk of multiple account holdings by a single customer. Customers are also required, at this stage, to disclose any status as Politically Exposed Persons (PEPs).

Following the initial deposit, the customer's details are automatically screened against updated PEP and Financial Sanctions lists to identify any potential high-risk indicators. A thorough evaluation of the customer's risk profile is then conducted, considering all previously gathered information and relevant risk factors. Ongoing monitoring is assigned based on the customer's risk classification (low, medium, or high).

All CDD activities — from identity verification to ongoing risk assessments — are carefully documented and securely retained for as long as the business relationship remains active. Additionally, these records are preserved for at least five years after the relationship ends, in full compliance with regulatory obligations, or longer if necessary following the filing of a Suspicious Transaction Report (STR).

Customer Due Diligence is systematically triggered in specific cases:

- When cumulative deposits linked to a customer reach NAF 4,000 (€2,000) over a rolling period.
- When preliminary screening flags a customer as potentially high-risk.
- When additional nationality or place of birth information is required.

Identity and address verification are performed through trusted verification service providers, cross-referencing customer data with reputable databases to ensure authenticity.

The documentation required for verification includes:

- A valid, unexpired government-issued photo ID (passport, national ID card, residence permit, or driving license).
- Proof of residential address, such as a recent bank statement, utility bill, official police certificate, or government-issued correspondence indicating the declared address.
- Proof of source of funds, including recent bank statements, images or scans of payment cards, or records from licensed E-wallet providers showing clear ownership of the funding method.
- A source of wealth declaration, which may be supported by employment contracts, salary slips, or relevant financial statements illustrating the origin of the customer's assets.

Through these enhanced, structured measures, the Company ensures a strong foundation for regulatory compliance, effective risk management, and the maintenance of a secure operational environment.

4.1 Enhanced Due Diligence

If a customer is classified as high-risk, the Company is required to implement a series of Enhanced Due Diligence (EDD) measures to rigorously verify the customer's identity, assess the legitimacy of their financial background, and mitigate potential risks:

- Additional, more stringent identity verification steps must be carried out. These include:
 - Acquiring a certified copy of the customer's identification document, authenticated by a reputable professional (such as a notary, lawyer, or accountant), whose professional status can be independently verified.
 - Conducting an independent cross-check of the customer's identity details against a second reliable electronic verification source to confirm consistency and authenticity.

Source of Wealth (SOW) Verification

- The Company must thoroughly validate the origin of the customer's wealth, demanding verifiable evidence rather than relying solely on self-declarations. Acceptable forms of evidence include:
 - **Employment or Business Income:** Recent payslips, employer-issued confirmation letters, or up-to-date audited financial statements for business owners.
 - **Real Estate Transactions:** Executed copies of property sale contracts or official land registry extracts.
 - **Inheritance:** Legal copies of wills, probate documents, or inheritance settlement statements detailing the value and distribution.
 - **Corporate Sales:** Sale agreements, financial documentation from certified accountants, or formal declarations from legal representatives confirming the proceeds of business sales.

Source of Funds (SOF) Verification

- The precise origin of the customer's funds must be verified to ensure they are not sourced from unlawful activities. Deposits should originate from payment instruments issued by financial institutions licensed within the European Economic Area (EEA) or similarly regulated jurisdictions.

Communication with Payment Service Providers

- Where possible, the Company should establish direct communication with the financial institution or payment service provider responsible for the customer's deposit method to obtain additional assurances regarding the customer's reliability and transactional integrity.

Enhanced Due Diligence for Politically Exposed Persons (PEPs)

- In cases where the customer is identified as a PEP, a thorough reputational review must be conducted. This includes evaluating any adverse media coverage, public records, and other relevant information to determine how the PEP's status may impact the risk exposure of the ongoing business relationship.

Through the careful application of these additional procedures, the Company strengthens its controls to prevent exposure to Money Laundering (ML) and Financing of Terrorism (FT) risks associated with high-risk customers.

5. Sanctions

Customers are granted a period of thirty (30) days to fully satisfy the Company's Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) requirements. During this window, based on the customer's risk profile and pending verification status, temporary restrictions may be imposed on the customer's account. Such restrictions can include limiting access to certain deposit or withdrawal methods, capping transaction amounts, or restricting the use of deposited funds for gameplay or other services until the verification is completed.

If, at the end of the thirty (30) day period, the customer has not provided the necessary documentation or information to the satisfaction of the Company, the customer will be deemed to have failed the due diligence process. In these cases, the Company reserves the right to immediately suspend or permanently close the customer's account in accordance with its regulatory obligations.

Should the customer be assessed during this period as posing a potential high risk of Money Laundering (ML) or Financing of Terrorism (FT), the Company will escalate the matter internally and may file a Suspicious Transaction Report (STR) in accordance with its established Internal Suspicious Transaction Reporting Procedure. All subsequent business activities and transactions with the customer will be frozen unless specific clearance or further guidance is received from the relevant Financial Intelligence Unit (FIU) following the STR submission.

Where a customer has failed to meet CDD/EDD obligations within the prescribed timeframe but has not been flagged as a potential high ML/FT risk, the Company will proceed to close the account as a precautionary measure. Any funds remaining in the account at the time of closure will be returned to the customer, whenever possible, using the same deposit method originally utilized. Where the original payment method is no longer available or practical, additional verification may be required to process the refund securely.

In all cases, the Company ensures that actions taken following the expiry of the 30-day period are meticulously recorded, along with the rationale behind the account closure or reporting decisions, in line with its internal recordkeeping policies and applicable legal obligations.