

Mr. Cedric Pietersz
Curaçao Gaming Authority
Scharlooweg 172-174
Willemstad-Curaçao

30 May 2025

Re: Uploading AML/CFT Policy

Dear Mr. Pietersz,

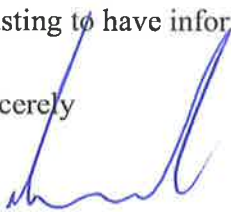
In order to comply with the due date for submission of the AML/CFT Policy, the applicant hereby uploads the draft version of the AML/CFT policy.

Note that this policy is not yet final as it is under review by management for approval and sign off.

Once approved, the final and official version will be signed off by management and uploaded to the portal. We expect this to take place in the course of the coming week.

Trusting to have informed you accordingly.

Sincerely



Raoul Behr
Managing Director

Anti-Money Laundering, Counter-Terrorism Financing and Counter-Proliferation Financing Policy

Frontier Gaming B.V.

APPROVAL:

DATE:	MAY 30, 2025
NAME AND AUTHORITY:	
SIGNATURE:	

DOCUMENT INFORMATION:

APPROVAL	BOARD OF DIRECTORS
RESPONSIBLE OFFICE	COMPLIANCE OFFICER
REVIEW	ANNUALLY
AUDIENCE	ALL EMPLOYEES, CONTRACTORS, AND THIRD PARTIES
EFFECTIVE DATE	APRIL 10, 2025
NEXT REVIEW DATE	MAY 30, 2026

Table of Contents

1.	POLICY STATEMENT	5
2.	PURPOSE.....	6
3.	DEFINITIONS.....	8
4.	POLICY IMPLEMENTATION	10
4.1	RESPONSIBILITY OF THE SENIOR MANAGEMENT	10
4.2	DISTRIBUTION OF THE AML POLICY	10
4.3	APPOINTMENT OF THE COMPLIANCE OFFICER.....	11
4.4	REPORTING STRUCTURE AND INDEPENDENCE	11
4.5	DUTIES AND RESPONSIBILITIES OF THE COMPLIANCE OFFICER	12
5.	BUSINESS RISK ASSESSMENT	14
6.	CUSTOMER RISK ASSESSMENT	14
7.	CUSTOMER ACCEPTANCE POLICY	16
7.1	PROHIBITED CATEGORIES OF CUSTOMERS	16
7.2	RISK INDICATORS.....	16
7.3	CUSTOMER DUE DILIGENCE MEASURES (CDD).....	17
7.4	POLITICALLY EXPOSED PERSONS (PEPs)	17
7.5	SANCTIONS SCREENING.....	18
8.	CUSTOMER DUE DILIGENCE	19
8.1	CUSTOMER DUE DILIGENCE MEASURES.....	19
8.2	ENHANCED DUE DILIGENCE (EDD).....	21
8.3	POLITICALLY EXPOSED PERSONS (PEPs)	22
8.4	TARGETED FINANCIAL SANCTIONS	23
8.5	TIMELINE FOR COMPLIANCE AND NON-COMPLIANT DOCUMENTS	24
9.	ONGOING AND CONTINUOUS MONITORING	25
9.1	ONGOING CUSTOMER PROFILE MONITORING	25
9.2	ONGOING TRANSACTION MONITORING.....	25
10.	REPORTING OF UNUSUAL TRANSACTIONS	26
10.1	INDICATORS OF UNUSUAL TRANSACTIONS	27
10.2	PROHIBITION OF DISCLOSURE	28
10.3	PROTECTION FOR REPORTING EMPLOYEES	28
10.4	RECORD KEEPING.....	28
11.	AML COMPLIANCE PROGRAM.....	29
11.1	EMPLOYEE DUE DILIGENCE	29
11.2	TRAINING	30
11.3	INDEPENDENT AML AUDIT.....	31
11.4	EXAMINATION BY THE GAMING CONTROL BOARD.....	31
12.	COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE.....	32

13. CONTACT INFORMATION..... 34

14. POLICY HISTORY 34

15. ANNEX I: CUSTOMER RISK ASSESSMENT TEMPLATE 35

16. ANNEX II: INTERNAL UNUSUAL TRANSACTION REPORT 36

17. ANNEX III: GEOGRAPHICAL RISK CLASSIFICATION 39

1. POLICY STATEMENT

Frontier Gaming N.V. (hereinafter the “Company” or “FANPLAY”) is registered in the Commercial Register of the Curaçao Chamber of Commerce & Industry under registration number 165948 with registered address Emancipatie Boulevard, Dominico F. "Don" Martina 31, Willemstad, Curaçao. Frontier Gaming N.V. is a licensed operator of offshore games of chance under license number OGL/2024/1055/0507 from the Curaçao Gaming Authority, operating FANPLAY.GG.

The Company is fully committed to preventing money laundering (ML), terrorist financing (TF) and the financing of proliferation of weapons of mass destruction (PF) activities within its operations. In alignment with relevant laws and regulations, the Company will establish and maintain comprehensive policies and procedures to ensure compliance and mitigate risks associated with these activities.

This Anti-Money Laundering and Terrorist Financing Policy (hereinafter referred to as the "Policy") applies to all employees of the Company, including full-time and contractual staff, across all departments and functions, and relevant third parties. The Policy outlines the Company's commitment to creating a secure environment that actively discourages the misuse of its services for illegal purposes.

The objectives of this Policy are as follows:

1. Ensure that FANPLAY adheres to all applicable laws, regulations, and statutory instruments related to anti-money laundering and terrorist financing.
2. Safeguard FANPLAY and its employees from the risks associated with breaches of law and regulatory requirements, including potential legal repercussions.
3. Protect FANPLAY's reputation from the risks of being implicated in money laundering or terrorist financing activities, thereby maintaining public trust and confidence.
4. Make a positive impact in the ongoing global fight against crime and terrorism by implementing robust measures to prevent the misuse of FANPLAY's services.

2. PURPOSE

The purpose of this Policy is to ensure the Company's compliance with the relevant legal and regulatory requirements from the authorities in charge of the supervision of AML, CTF and CPF matters for the gaming sector are the CGA and the Curaçao Financial Intelligence Unit (FIU), while simultaneously ensuring the integrity and sustainability of the operations of the Company.

The following laws and regulations, as well as any additional regulations issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law, are applicable to the Company:

- Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6.;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- National Decree for general measures, of the 10 July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10 July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30);

- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Ordinance of the 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157);
- Curaçao Gaming Control Board Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025.

By fostering a culture of compliance, transparency, and accountability at all levels of the organization, the Company aims to create an environment where everyone understands the importance of adhering to these obligations. Additionally, the Policy implements a risk-based strategy for Customer Due Diligence, Ongoing Monitoring, and the Reporting of Unusual Transactions, ensuring that resources are allocated efficiently to address potential risks.

From a business perspective, this Policy is essential for protecting the integrity of the Company's operations. By preventing misuse by criminal elements, the Company can maintain a secure environment for its customers and stakeholders. Furthermore, the Policy helps preserve the Company's reputation with customers, financial institutions, and regulatory bodies. Demonstrating compliance is crucial for retaining operating licenses and fostering successful business partnerships. Moreover, by mitigating legal, financial, and operational risks associated with AML/CTF violations, the Policy supports overall business continuity.

The Company recognizes that effective prevention of ML and TF requires active engagement from all employees. To facilitate this, the Company will provide comprehensive training in anti-money laundering protocols and procedures, equipping staff with the necessary knowledge and skills to identify and report unusual activities.

3. DEFINITIONS

Key definitions include:

CFATF means the Caribbean Financial Action Taskforce. An organization of twenty-four (24) states of the Caribbean Basin, Central and South America, which have agreed to implement common countermeasures to address money laundering.

Compliance Officer means a senior officer at management level and independent from the games' operations, responsible for the detection and deterrence of money laundering and terrorist financing.

Customer Due Diligence or **CDD** means the process of identifying and verifying customers and assessing their risk.

FATF means the Financial Action Task Force. An independent intergovernmental body, established in 1989 and mandated by its Member Jurisdictions to develop and promote policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

FATF Recommendations means a framework of recommendations on policies and measures, issued by the FATE, to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction;

Financial Transactions means deposits and withdrawals (bonusses are not included). Amounts wagered and winnings are considered as gambling transactions. Gambling transactions are not considered as financial transactions.

FIU means the Financial Intelligence Unit Curaçao, referred to in art. 2 of the NORUT.

Kingdom Sanctions Act means the National Ordinance also known as the "Rijkssanctiewet", published under N.G. 2016 no. 54.

NOIS means National Ordinance on Identification of Clients when rendering Services (Landsverordening identificatie bij dienstverlening, N.G. 2017, no. 92).

NORUT means National Ordinance on the Reporting of Unusual Transactions (Landsverordening Melding Ongebruikelijke Transacties, N.G. 2017, no. 99).

Money Laundering or **ML** means the process of disguising the illicit origin of funds.

Politically Exposed Persons or **PEPs** means individuals who are or have been entrusted with prominent public functions by a foreign country and the direct family members or close associates of such persons. Examples are: Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

Sanctions National Ordinance means the National Ordinance also known as the “Sanctielandsverordening”, published under N.G. 2014 no. 55.

Source of Funds refers to how the funds for a particular transaction were obtained by the player, like personal savings, pension release, property sales, share sales and dividends, gambling winnings, gifts, compensation from legal rulings.

Source of Wealth means the origin of all the money a person has accumulated over their lifetime, like employment income, inheritances, investments, business ownership interests.

Terrorist Financing or **TF** means providing funds for terrorist activity or organizations.

Unusual transaction means a transaction that is considered as such on the basis of certain indicators, pursuant to Article 10 of the NORUT.

Ultimate beneficial ownership or **UBO** means the natural person who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person.

4. POLICY IMPLEMENTATION

Policy implementation involves a risk-based approach to detect and mitigate ML/TF/FP risks. It includes Business Risk Assessment, Customer Risk Assessment, Customer Acceptance Policies, Due Diligence procedures, Ongoing Monitoring, and Reporting mechanisms. Detailed processes and responsible departments are outlined in the sub-sections below.

4.1 Responsibility of the Senior Management

The Senior Management is responsible for:

- setting and approving the general principles underlying the Policy for Prevention and Combatting of Money Laundering and Terrorist Financing;
- appointing Compliance Officer and Deputy Compliance Officer and communicating to them the internal policies;
- defining the duties and responsibilities of the Compliance Officer;
- ensuring that effective and sufficient systems and controls are in place to enable compliance with all rules and regulations;
- ensuring that the Compliance Officer has completed and timely access to all data required to effectively undertake their duties including, but not restricted to, data concerning customer identity, transaction documentation and other relevant information maintained;
- ensuring that all employees are aware to whom they have to report any information concerning unusual transactions;
- ensuring that the Compliance Officer has sufficient resources including competent staff and technological equipment;
- assessing and approving the annual report and taking appropriate actions to remedy any weaknesses and/or deficiencies identified in the annual report.

4.2 Distribution of the AML Policy

The Senior Management Team has reviewed and approved this AML Policy. The Policy is delivered to all staff members, including frontline workers, team leaders, managers, and the Board. It is also reissued and redistributed whenever updates are made.

One of the primary responsibilities of the Compliance Officer, is to submit a report to the Executive Management team for assessment at least once every twelve (12) months. This report evaluates the efficiency of the Policy and its associated operational procedures. Additionally, the Compliance Officer is expected to offer recommendations to management regarding potential improvements to operational processes or policies.

The Compliance Officer will conduct a thorough assessment of this Policy at least once every twelve (12) months to identify any necessary adjustments or updates.

With the exception of directives from relevant authorities, any proposed amendments to the Policy require the review and approval of the Compliance Officer, Senior Management, and legal counsel.

4.3 Appointment of the Compliance Officer

It is imperative that a suitably experienced senior staff member be designated as the Compliance Officer at all times. The individual responsible for ensuring compliance has been designated and their contact information has been made accessible to all employees and relevant personnel from service providers.

4.4 Reporting Structure and Independence

The Compliance Officer holds no other position within the organization and operates independently from all other functions within the organization in order to ensure that actual or perceived conflicts of interest do not occur.

The Compliance Officer possesses the autonomy to operate autonomously from other departments within the organization in order to effectively carry out the specific duties and obligations outlined below.

The Compliance Officer has the full and public support of the executive management team in executing their duties. All staff are required to assist the Compliance Officer (and/or the nominated officer, as appropriate) in fulfilling their duties.

4.5 Duties and Responsibilities of the Compliance Officer

- Design and Implementation of the AML Program: Design and implement the Company's Anti-Money Laundering (AML) program to ensure effective prevention and detection of money laundering and terrorist financing activities.
- Compliance with Laws and Regulations: Ensure compliance with Curaçao laws and regulations regarding money laundering and terrorist financing, as well as all applicable legislation, regulations, guidelines, codes of practice, and Company policies and procedures.
- Oversight and Management: Oversee and manage all compliance-related functions within the Company and its affected suppliers, including the protocols described in this Policy.
- Review of Policies and Procedures Adherence: Review adherence to the Company's policies and procedures and ensure they are effectively implemented.
- Transaction Analysis: Analyze transactions and identify those subject to reporting under the Ministerial Decree on Indicators for Unusual Transactions.
- Review of Unusual Transactions: Review internally reported unusual transactions for completeness and accuracy.
- Record Maintenance: Maintain records of both internally and externally reported unusual transactions.
- Internal Procedures for Reporting: Design and implement internal procedures regarding when the reporting of unusual transactions will lead to blocking or freezing of user accounts.
- Investigation of Unusual Transactions: Conduct further investigations into unusual transactions as necessary and report findings to senior management.
- External Reporting: Prepare external reports on unusual transactions as required by regulatory authorities.
- Training Coordination: Plan and coordinate training sessions for all departments on compliance-related issues, including key regulatory areas such as ID and age verification, fraud prevention, anti-money laundering, and problem gambling.
- Reporting to Management: Report to the CEO and inform senior management of the results of any remedial actions taken regarding compliance issues. Prepare periodic reports on the Company's efforts

against money laundering, terrorist financing, and proliferation financing to be submitted to senior management.

- Consultation with Staff: Consult with staff representatives and attend staff meetings on compliance topics to ensure awareness and understanding of compliance obligations.
- Monitoring of Internal Controls: Manage regular reviews of the Company's internal control systems to ensure they accurately reflect the current operations of the business and report any discrepancies to relevant senior management.
- Continuous Improvement: Stay informed about local and international developments related to money laundering and terrorist financing, and suggest improvements to management regarding the AML program.

5. BUSINESS RISK ASSESSMENT

The Business Risk Assessment (BRA) framework is a crucial component of the Company's AML, CTF, and CPF compliance program. It provides a systematic, risk-based approach for identifying, assessing, and mitigating money laundering, terrorist financing, and proliferation financing risks within the Company's operations.

The Company performs thorough BRAs, evaluating potential risk factors related to customers, products and services, geographic locations, and delivery channels. Each risk factor is assessed for its likelihood and potential impact. Tailored controls and measures are then implemented to address these risks. All findings, evaluations, and mitigation strategies are documented and reported to senior management and relevant regulatory authorities.

BRAs are conducted regularly to maintain an accurate risk profile, with comprehensive assessments performed annually. Additional assessments may be triggered by significant events, such as the introduction of new products, regulatory changes, or major shifts in the business environment.

6. CUSTOMER RISK ASSESSMENT

The Customer Risk Assessment procedure is a crucial component of the internal AML program at the Company, designed to evaluate the specific risks associated with providing services or products to customers.

The assessment begins when a new customer applies for an account, at which point their risk profile is formulated based on the information collected. The initial Customer Risk Rating assigned helps determine the frequency and intensity of ongoing reviews; higher-risk customers will be subject to more frequent and rigorous monitoring.

The assessment process considers several key factors:

- **Customer Risk:** This involves evaluating the customer's background, occupation, and transaction patterns. Higher-risk categories include customers with multiple or irregular income sources, politically exposed persons (PEPs), high spenders, disproportionate spenders (whose spending habits do not align with their known income), and those using third parties to gamble in ways that may circumvent customer due diligence measures.

- **Product/Service Risk:** This factor assesses the risks associated with the Company's offerings. Certain gaming products or services, especially those allowing customers to influence outcomes, pose higher risks. Payment methods are also evaluated, with specific high-risk factors including anonymous payment options (like pre-paid cards and virtual assets), unusual account usage, peer-to-peer gaming, and multiple accounts or wallets. Additionally, identity fraud and the use of unlicensed electronic wallets are considered significant risks.
- **Geographic Risk:** The geographic location of the customer and the transaction is assessed, with higher risk assigned to customers from countries with weak AML regulations or high corruption levels. Relevant sources of information include the FATF lists of high-risk jurisdictions, the U.S. Department of State's International Narcotics Control Strategy Report, and other credible indices. The nationality, residence, and place of birth of the player are also taken into account.
- **Delivery Channel Risk:** This involves evaluating the methods used to establish a business relationship or conduct transactions. Channels that favor anonymity and non-face-to-face interactions are considered higher risk, prompting the Company to implement reasonable measures to mitigate these risks.

After the assessment, customers are categorized as low, medium, or high risk. The level of due diligence and ongoing monitoring applied corresponds to their risk classification:

- For customers assessed as **low risk**, a Simplified Due Diligence process will be applied, provided they do not exhibit any risk-enhancing characteristics and their transactions remain below the threshold of Cg. 4,000.
- **Medium risk** customers will require additional information and documentation in accordance with the Company's policies.
- **High risk** customers will be subject to Enhanced Due Diligence in line with this Policy, and applicable mitigation measures shall be adopted;
- Accounts classified as extremely high risk or displaying potentially unusual behavior will be reviewed by compliance personnel and reported to the Compliance Officer (CO) for further investigation.

This structured approach ensures that the Company effectively identifies and mitigates the risks associated with its customers, aligning with regulatory expectations and promoting a robust AML compliance program.

7. CUSTOMER ACCEPTANCE POLICY

The Company's Customer Acceptance Policy (CAP) is designed to ensure compliance with legal requirements while aligning with the Company's risk appetite and Business Risk Assessment (BRA). The CAP outlines the criteria for accepting customers, identifies higher-risk individuals, and delineates the necessary Customer Due Diligence (CDD) measures to mitigate risks associated with money laundering (ML), terrorist financing (TF), and proliferation financing (PF).

7.1 Prohibited Categories of Customers

The Company will not accept customers who fall into the following categories:

- Individuals under the age of 18.
- Individuals listed on sanctions imposed by the UN, EU, or OFAC.
- Individuals with reasonable grounds to suspect involvement in ML, TF, PF, or any other criminal activity.
- Self-excluded customers who are barred from accessing our platforms or included in national self-exclusion registers as required by licensing conditions.
- Individuals who provide documents or information that the Company suspects to be fraudulent or falsified.

7.2 Risk Indicators

The following risk indicators will be used to categorize customers as low, medium, or high risk:

- Low Risk: Customers with stable income sources, consistent transaction patterns, and no red flags.
- Medium Risk: Customers with occasional irregularities in income or spending patterns, but no clear indications of criminal activity.
- High Risk: Customers with multiple income sources, irregular income streams, high spenders, disproportionate spenders, PEPs, and those using third parties to gamble or exhibiting unusual behaviors.

7.3 Customer Due Diligence Measures (CDD)

The level of CDD measures will be proportional to the risk classification:

- **Low and Medium Risk:** Simplified Due Diligence procedures will be applied, provided that the customer does not display any risk-enhancing characteristics and transactions remain below the threshold of Cg. 4,000.
- **High Risk:** Enhanced Due Diligence measures will be implemented, which include collecting additional information and documentation. For high-risk customers, ongoing monitoring will be more rigorous, including transaction reviews and alerts for unusual activity.

7.4 Politically Exposed Persons (PEPs)

The Company implements robust procedures for identifying and managing relationships with PEPs, defined as individuals entrusted with prominent public functions, as well as their close associates and family members.

- **Identification:** Comprehensive screening against reliable databases will be conducted during the onboarding process to determine PEP status.
- **Approval Process:** No business relationship shall be established or continued with a PEP without obtaining senior management approval.
- **Source of Wealth and Funds:** The Company will request a statement from the PEP regarding their source of wealth and verify this information through independent and reliable sources. Additional documentation may be requested if necessary.
- **Enhanced Monitoring:** The Company will conduct enhanced ongoing monitoring of PEPs, analyzing their spending patterns to ensure they align with declared legal sources of funds.

PEP status screening will occur regularly throughout the business relationship. If a customer not identified as a PEP at onboarding later becomes one, the Company will implement enhanced due diligence measures within 30 days. Failure to implement these measures will result in the termination of the relationship with that customer.

7.5 Sanctions Screening

The Company is committed to complying with targeted financial sanctions, which require the freezing of funds and assets of individuals and entities identified by the UN and EU as involved in terrorism or proliferation activities.

- **Ongoing Monitoring:** The Company will perform ongoing sanctions screening at key points, including during registration, withdrawal requests, and any changes to personal details or payment methods.
- **Action on True Matches:** If a true match is discovered and confirmed by the Compliance Officer, the Company will immediately freeze the funds of the affected customer and file a report with the Financial Intelligence Unit (FIU). Services will be terminated upon confirmation of the true match or earlier by the supervisory authority, and frozen assets will be held until further instructions are received.

8. CUSTOMER DUE DILIGENCE

8.1 Customer Due Diligence Measures

The Company is required to perform (CDD) under specific circumstances to ensure compliance with AML regulations and to protect the integrity of its operations. The Company must undertake CDD measures when players engage in financial transactions that amount to Cg. 4,000 or more. This includes any deposits or withdrawals made by the player.

Furthermore, if there is any suspicion of money laundering or terrorist financing, the Company is obligated to conduct CDD. This also applies in situations where there are doubts about the accuracy or completeness of previously obtained identification information from the player.

To effectively monitor and determine when a player reaches the Cg. 4,000 threshold for CDD purposes, the Company will evaluate not only individual transactions but also any series, combination, or pattern of transactions that exceed this amount. This evaluation will be conducted daily and will include all deposits, withdrawals, and peer-to-peer transfers made by the player.

Moreover, the Company maintains a strict Policy against anonymous accounts or accounts held under fictitious names. The company is committed to identifying each player by collecting their name and other relevant information, which is essential for determining the purpose and nature of the business relationship.

The Company's CDD procedures require prospective customers identify themselves by creating a profile at the point of registration. Mandatory information required at registration stage includes:

- Full name;
- Date of birth;
- Permanent residential address.

Once the above threshold of Cg. 4,000 is reached or any of the other triggers mentioned above, the customers are also required to provide their place of birth, nationality and identity number.

To fulfil the necessary customer identification and verification process, FANPLAY requires its customers to upload on their websites (under My profile → KYC) a copy of valid identification documents. This request is communicated to the customer via the email address registered. To complete the required customer verification process, the Company asks its customers to upload a copy of valid identification documents. Accepted identification documents include passport, identity card, driver's license or an equivalent document. This request is sent to the customer's registered email address (or other means of contact). If the documents are in a different language, the Company will take necessary steps to ensure that the documents adequately prove the customer's identity, such as obtaining a translation of the relevant parts. This may involve asking the customer to submit documents with a certified true translation.

Only documents issued by government agencies that include a photograph are deemed reliable for verifying the customer's identity. Government-issued documents that lack a photograph can be used to confirm the customer's current address, provided the address is included in the document. the Company accepts as proof of permanent residential address copy of utility bill (e.g. electricity, water, gas, telephone landline) or bank statements, as long as they are not older than 6 months at the time they are received.

When CDD checks on an existing customer have been completed within one of FANPLAY's products, CDD will not be conducted again in relation to another product unless a different payment method is used by the customer.

The Company is legally obligated to identify and verify the beneficial owner by confirming that customers are registering accounts to play and transact solely on their own behalf. We are committed to actively monitoring player activity to detect any instances where a player may be using the account to play on behalf of others. To effectively manage this responsibility, the Company has implemented the following safeguards designed to prevent access to our services by individuals deemed suspicious. These safeguards include:

- Payment Method Verification: Ensuring that the payment method used for deposits is in the name to the player, insofar as possible.
- Denial of Service: Preventing transactions for players attempting to use payment methods not in their own name.
- Withdrawal Identity Verification: Confirming the identity of players before processing withdrawals.

8.2 Enhanced Due Diligence (EDD)

In specific instances, it is possible for certain client relationships to exhibit elevated risks related to Anti-Money laundering (AML) or fraudulent activities, which may pose a potential threat to the Company. In such circumstances, alongside its customary client due diligence procedures, the Company will conduct enhanced due diligence (EDD).

During the enhanced due diligence process, the Company will take additional required steps in order to aid in identifying a potential customer, including (but not limited to) personal and financial background. This may involve obtaining additional evidence in verifying the individuality of the client.

The circumstances that always require Enhanced Due Diligence (EDD) are noted as follows:

- Customers or potential customers residing in jurisdictions associated with higher levels of corruption or inadequate AML, CTF, and CPF regulations.
- Politically Exposed Persons (PEPs), individuals who hold prominent public positions or are closely connected to such individuals, which may elevate the risk of corruption.
- Services or products that allow for a higher degree of anonymity, potentially facilitating illicit activities.
- The introduction of new services, technologies, or delivery mechanisms that may present unforeseen risks.
- Instances of account activity that may exhibit notable deviations from previously recognized patterns.
- Any other circumstances as Company reasonably perceives to be a heightened risk money laundering or terrorist financing.

The measures applied during EDD must align with the identified risks and may include, but are not limited to:

- Collect comprehensive information about the customer, including occupation, previous addresses, and relevant data from public databases and online resources.
- Obtain further information regarding the intended nature of the business relationship to better understand the customer's gaming habits and expectations.
- Gather detailed information on the source of funds or wealth for the player. In higher-risk situations, the Company will periodically request SOF information,

even if there has been no change in the customer's activity pattern. This ongoing diligence is essential for proactively addressing any potential concerns.

- Ask for information regarding the reasons for intended or performed transactions to ascertain their legitimacy and ensure they align with the customer's profile.
- Require approval from senior management before commencing or continuing the business relationship with higher-risk customers.
- Implement increased scrutiny of the business relationship, which may involve more frequent reviews of transactions and account activities.
- Require that the initial payment is made through an account in the customer's name with a bank that adheres to similar CDD standards.

8.3 Politically Exposed Persons (PEPs)

A PEP or Politically Exposed Person, is an individual who currently or previously held a prominent public function in any country. A PEP is an individual who is entrusted with a prominent public function, other than middle ranking or more junior officials, including but not limited to the following individuals:

- heads of state, heads of government, ministers and deputy or assistant ministers,
- members of parliament or of similar legislative bodies,
- members of the governing bodies of political parties,
- members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances,
- members of courts of auditors or of the boards of central banks,
- ambassadors, chargés d'affaires and high-ranking officers in the armed forces,
- members of the administrative, management or supervisory bodies of state-owned enterprises
- directors, deputy directors and members of the board or equivalent function of an international organization.

The following individuals are also regarded as PEPs by virtue of their relationship or association with the individuals listed above:

- family members of the individuals listed above, including spouse, partner, children and their spouses or partners, and parents
- known close associates of the individuals listed above, including individuals with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relations, or who is a sole beneficial owner of a legal entity or arrangement set up for the benefit of the PEP.

A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold.

In accordance with the risk-based approach that the Company employs, measures are tailored to the risk of the PEP, where the following are taken into consideration:

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

PEP status screening will be conducted regularly throughout the business relationship. If an account is identified as a potential match to a PEP list, the account shall be immediately frozen pending escalation and review. The Compliance Officer is immediately notified and a further assessment is made. The Compliance Officer will reach out to the appropriate department and offer his/her recommendations regarding the account. If a player who was not identified as a PEP at onboarding later becomes one, the Company is required to implement the enhanced due diligence measures within a thirty-day window of this determination. Failure to implement the required measures for newly identified PEPs within the specified timeframe will result in the termination of the relationship with that customer.

8.4 Targeted Financial Sanctions

The Company is committed to complying with targeted financial sanctions, which require the freezing of funds and assets of individuals and entities identified by the United Nations (UN) and European Union (EU) as being involved in terrorism or proliferation activities. Mechanisms are established to ensure compliance with the Company's legal obligations. This includes, but is not limited to, the following:

- The Company shall comply with relevant sanctions decrees and regulations and monitor any and all amendments thereof and implement these without undue delay.
- The Company shall perform ongoing sanctions screening on customers and also perform trigger-based sanctions screening of customers at least in the following scenarios:
 - At the moment of registration;
 - At the moment of withdrawal request;
 - At the moment of any request for change of personal details or payment methods.

In the event that a true match is discovered and confirmed, the Company must follow the established Process for the freezing of resources as per the Sanctions Ordinance, and must immediately file a report with the FIU.

8.5 Timeline for Compliance and Non-Compliant Documents

If the customer cannot provide compliant documents within 30 days from the moment the Cg. 4,000 threshold is reached, the Company shall terminate the relationship with the customer and consider filing an Unusual Activity Report with the FIU.

During the CDD process, customers may continue to access their accounts while the Company gathers the necessary information. However, if a deposit reaches the Cg. 4,000 threshold, the customer will be prohibited from further deposits or withdrawals, although they may continue to play with their existing balance. Conversely, if the threshold is reached due to a withdrawal request, the account will be completely frozen, halting all gameplay.

If a document submitted by a (potential) customer does not meet the verification standards, the compliance officer or designated staff member must immediately flag it for further examination. The initial review should be thorough to pinpoint the specific reasons for non-compliance. Once a non-compliant document is identified, the customer must be informed without delay.

All actions taken in response to non-compliant documents shall be carefully recorded. This includes the initial identification of the issue, communications with the customer, any

escalations, and the final outcome. Comprehensive records should be maintained in the customer's file to ensure a complete audit trail.

9. ONGOING AND CONTINUOUS MONITORING

The Company implements and monitors all activity of clients to ensure that all activity whether it be transactional or instructional, be consistent and given the required attention for the detection of possible money laundering or terrorist financing.

9.1 Ongoing Customer Profile Monitoring

During the periodic review of a customer, the Company verifies and confirms that the CDD information about the client, nature and purpose of the business relationship, and SOF is still accurate and up to date, evaluate if there are external signals (i.e. bad press/adverse news, incidents) that could give rise to a change in the business risk profile of the customer and ensure to perform screening against sanctions lists and PEP lists. The periodic review also includes an overall review of the transaction behaviour of the client to determine if unusual activities have taken place, for instance in case of transactions which normally would not be expected.

The periodic review of the customer is based on the risk profile of the customer:

- For high-risk customers – once per year;
- For medium risk customers – once every 2 years;
- For low-risk customers – once every 3 years.

9.2 Ongoing Transaction Monitoring

The Company performs both real-time monitoring of transactions, as well as post-event monitoring, to ensure that such transactions and activity are consistent with the Company's knowledge of the client and their expected activity. More attention is paid to high amounts, high-risk clients and high-risk jurisdictions.

Particular risk factors will be closely monitored concerning business relationships and transactions, including:

- Gambling or transaction patterns that diverge from what is considered normal or what the customer initially indicated when establishing the business relationship.
- Execution of unusually large transactions by the customer.
- Requests for withdrawals to accounts other than those verified to belong to the customer (such withdrawals are prohibited).
- Requests to transfer gambling accounts or winnings to third parties (such transfers are also prohibited).

10. REPORTING OF UNUSUAL TRANSACTIONS

The Company is committed to identifying and reporting any unusual activities and transactions, including attempted transactions, to ensure compliance with Anti-Money Laundering (AML) regulations. This section outlines the procedures and responsibilities for recognizing, reporting, and investigating unusual transactions.

Employees must report any unusual activity to the Money Laundering Reporting Officer (MLRO) immediately, but no later than 24 hours after the transaction has been executed. This includes any transactions that raise suspicion or deviate from normal behavior.

Employees must submit an Internal Unusual Transaction Report (IUTR) to the MLRO, in a format approved by Management. All additional documents available, such as copies of identification documents, cash out slips, and other records must be also submitted as supplements.

If a more in-depth investigation is required, the MLRO may request additional information from relevant departments. This investigation must be completed within ten (10) business days.

The Compliance Officer will assess the information available to determine if it is sufficient to warrant filing an Unusual Transaction Report (UTR) with the FIU Curaçao. If the Compliance Officer concludes that the activity is unusual, a report shall be submitted to the FIU regarding any unusual monetary operations or transactions within 48 hours.

10.1 Indicators of Unusual Transactions

The Company observes both objective and subjective indicators to assess whether a customer's transaction is deemed unusual. The following transactions or intended transactions are considered unusual:

Objective indicators

<i>A. A transaction which is reported to the police or judicial authorities</i>	
Indicator	Definition
G0000111	A transaction which is reported to the police or judicial authorities in connection with money laundering or the financing or terrorism.
<i>B. An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance.</i>	
G0000114	An intended transaction carried out by or for the benefit of a person, legal person, group or entity that is mentioned on a list compiled in pursuance of the Sanctions National Ordinance.
<i>C. A transaction amounting to NAF (ANG) 5,000.00 or more, regardless whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner; This comprises in any case the following situations:</i>	
G0000135	1. <i>A giro-based transaction amounting to NAF (ANG) 5,000.00 or more:</i> A giro-based transaction is a transfer from a bank account of the service provider to a local or international bank account carried out at the request of the client addressed to the service provider.
	2. <i>The taking into deposit or the releasing out of deposit of an amount of NAF(ANG) 5,000.00 or more, at the request of the client.</i>
	3. <i>Sale of tokens to a client in the amount of NAF (ANG) 5,000.00 or more.</i> The term "tokens" includes at least chips and credits.
	4. <i>Payout of prizes in the amount of NAF (ANG) 5.000,-- or more.</i>
	5. <i>All other cases.</i>
NB In case of Indicator G0000135: please also indicate the applicable sub-indicator (1,2,3,4 or 5) when reporting a transaction. In case of sub-indicator 5, please always provide a description of the situation.	

Subjective indicator

<i>Suspected money laundering transactions or financing of terrorism.</i>	
Indicator	Definition`
G0000211	A transaction giving cause to assume that it may be connected with money laundering or terrorist financing.

10.2 Prohibition Of Disclosure

All reports and investigations must be handled with the highest level of confidentiality in accordance with applicable laws and regulations. Unauthorized disclosure of information related to unusual activity reports is strictly prohibited and may lead to legal and disciplinary action.

10.3 Protection For Reporting Employees

The Company has implemented measures to safeguard employees and representatives who report suspicions of money laundering, terrorist financing, and/or financing of proliferation to the FIU. Employees reporting such suspicions are protected from threats or hostile actions by other employees, management, or customers, as well as from adverse or discriminatory employment actions

10.4 Record Keeping

The Company retains all necessary records of transactions, both domestic and international, for a minimum of five (5) years to ensure compliance with information requests from regulatory authorities. These records must be detailed enough to allow for the reconstruction of individual transactions, including the amounts and types of currency involved, if applicable, to provide evidence for potential criminal prosecutions.

All records gathered through CDD measures, such as copies of official identification documents, account files, and business correspondence, will be stored for at least five (5) years after the business relationship has ended or after the date of an occasional transaction.

Records shall be stored in a manner that ensures their integrity, confidentiality, and accessibility. Electronic records shall be stored in secure, encrypted databases with access controls to prevent unauthorized access. Physical records shall be stored in locked, fireproof cabinets within secure areas of the office. Access is restricted to authorized personnel only. Regular backups of electronic records shall be conducted and stored in a separate, secure location to prevent data loss.

After the retention period, records shall be disposed of securely to prevent unauthorized access or disclosure. Electronic records must be permanently deleted using secure deletion software that ensures data cannot be recovered. Physical records must be shredded using cross-cut shredders or incinerated to ensure complete destruction.

When properly ordered to do so by any enactment, rule of law or court order, the Company shall provide a document, customer due diligence information, or enhanced due diligence information and the Company will maintain a register of the documents and information provided and will keep a copy of the same.

11. AML COMPLIANCE PROGRAM

Monitoring the adherence of the Company's compliance program to legal and regulatory AML/CFT obligations, is a standard practice. Annual reviews of the Policy will be conducted, and amendments will be made in accordance with the application of new products and/or implementations.

11.1 Employee Due Diligence

Employee due diligence is a process to screen employees with the objective of identifying and reducing the Company's exposure to the risks associated with ML and TF. These procedures apply not only to the Company's contractual employees, but also to its contractors and subcontractors. The employee due diligence process is informed by the Company's risk assessment and the specific roles within the organization.

Any employee whose position may enable them to facilitate ML or TF must undergo screening. This requirement applies to prospective employees prior to their hiring for such roles, as well as current employees from time to time. Regular updates and re-evaluations are essential for maintaining an effective compliance program against ML, TF and PF.

To screen both current and potential employees, The Company will:

- Identify the individuals;
- Verify their identity;
- Confirm their employment history, such as through references; and

- Determine their suitability for the position and assess whether they pose any risk to the Company.

Positions that may render an employee vulnerable to collusion with or coercion by criminal organizations should undergo more rigorous checks. The Company must evaluate whether:

- The employee has a criminal record, which may be verified through a police check.
- The employee is or has been subject to regulatory, court, or legal actions.
- The employee has leveraged bankruptcy laws for personal gain.

11.2 Training

In delivering AML, CTF and CPF training to the designated categories of employees, the Company will consider the necessary knowledge and qualifications required for their duties, responsibilities, and authorizations. As part of the training framework, the Company will outline the AML, CTF and CPF requirements and provide comprehensive information on the measures and activities that staff are expected to undertake within their roles.

The Company will ensure that documentation of the training provided to staff is maintained, capturing the following information:

- Details on the content of the training programs;
- The names of the staff members who have received the training;
- The date on which the training was provided;
- The results of any testing carried out to measure staff understanding of money laundering and terrorist financing requirements; and
- An ongoing training plan.

The Company will regularly update the training programs to reflect any changes in internal and external regulations, as well as developments in the availability of training programs in the market for external training. Furthermore, extraordinary training in AML, CTF and CPF matters will be provided in specific situations, including:

- The introduction of new internal and external regulations related to AML, CTF and CPF that apply to the Company's staff.

- The launch of new products or services that alter the AML, CTF and CPF risk exposure.
- Instances where an employee breaches internal or external AML, CTF and CPF regulations due to a lack of knowledge during the performance of their duties.

11.3 Independent AML Audit

Periodically, the efficacy of the organization's AML/CFT program is assessed to ascertain that it remains pertinent and in accordance with industry standards, best practices, business operations, and regulatory advancements. The Company demonstrates compliance with all relevant legal and regulatory obligations in the jurisdictions where it conducts business.

An external independent qualified AML/CFT auditor will be engaged for the annual evaluation of the AML program, ensuring findings are documented. The audit must include several key assessments, such as:

- Reviewing the Company's AML, CTF and CPF manual.
- Examining customer files.
- Evaluating compliance management.
- Conducting transaction testing.
- Assessing the adequacy of training.
- Ensuring compliance with relevant laws and regulations.
- Evaluating the system's capacity to detect unusual activities.
- Interviewing employees involved in transactions and their supervisors.
- Sampling unusual transactions and reviewing compliance with internal and external policies and reporting requirements.
- Assessing the effectiveness of the record retention system.

The audit shall also evaluate the Company's responsiveness to previous audit findings. All testing scope and results must be documented, with any deficiencies reported to senior management, along with requests for prompt corrective actions.

11.4 Examination by the Gaming Control Board

The Company shall provide information and documentation regarding its money laundering and terrorist financing policies and procedures to examiners of the GCB during examinations or upon request. The following items must at all times be readily available and accessible:

- The written and approved AML Compliance Program addressing ML/TF/PF.
- Records of the Business Risk Assessment.
- The name and job description of the Compliance Officer responsible for the Company's AML policies and procedures.
- Records of reported unusual transactions.
- Records of unusual transactions that required further investigation.
- Records of frozen accounts.
- A schedule of training provided to personnel on ML/TF/PF.
- Assessment reports on the Company's policies and procedures regarding money laundering, terrorist financing, and proliferation financing from the internal audit department or an external auditor.
- Customer files, including risk assessments, CDD, customer acceptance, and transaction information.

12. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

The Company is fully committed to adhering to all applicable laws and regulations related to Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and sanctions enforcement as established by the jurisdiction of Curacao, aligning with international best practices, including the FATF Recommendations. Compliance with the AML/CTF Policy is mandatory for all employees, officers, agents, and third-party service providers. Non-compliance may expose the organization and individuals to significant legal, regulatory, and reputational risks, including fines or penalties imposed by Curacao's authorities, revocation or suspension of the Company's gaming license, and potential criminal prosecution for wilful violations.

Additionally, non-compliance can lead to reputational damage, resulting in loss of customer trust, negative media exposure, and strained relationships with financial partners. Operational disruptions may also occur, such as freezing of funds, loss of access to financial systems, and increased scrutiny from regulators.

Employees who violate the AML/CTF Policy may face disciplinary actions, including formal warnings, suspension, or termination for serious or repeated breaches, as well as potential referral to law enforcement. Third-party providers may have their agreements terminated if found non-compliant. All employees must understand and comply with the AML/CTF Policy,

participate in mandatory training, and report any unusual behavior or breaches to the Compliance Officer, who will ensure that whistleblower protections are in place.

The Compliance Officer and senior management are responsible for investigating violations, determining appropriate disciplinary actions, and reporting serious breaches to relevant authorities. All enforcement actions are documented and reviewed periodically to improve the compliance program.

13. CONTACT INFORMATION

For questions regarding this Policy, please contact Anna Glam, CAMS, Compliance Officer of Frontier Gaming B.V.

Email: anna@compliance-caribbean.com

Phone: (+599)9 461 7974

14. POLICY HISTORY

DATE	VERSION	SUMMARY CHANGES
JULY 16, 2024	1.0	POLICY IMPLEMENTATION
MAY 30, 2025	2.0	POLICY UPDATE IN LINE WITH CGA REGULATIONS

15. Annex I: Customer Risk Assessment Template

Customer Risk Assessment Template		
Customer Information		
Full Name		
Date of Birth		
Nationality		
Residential Address		
Occupation		
Source of Funds		
Risk Factor Evaluation	Risk Level (Low/Medium/High)	Comments
Customer Background		
Occupation		
Multiple/Irregular Income Sources		
Politically Exposed Person (PEP)		
High/Disproportionate Spender		
Third-Party Gambling		
Product/Service Risk Evaluation	Risk Level (Low/Medium/High)	Comments
Gaming Product Type		
Payment Method		
Peer-to-Peer Gaming		
Geographic Risk Evaluation	Risk Level (Low/Medium/High)	Comments
Country of Residence		
Country of Nationality		
Delivery Channel Risk Evaluation	Risk Level (Low/Medium/High)	Comments
Anonymity Factors		
Overall Risk Assessment:	Risk Level (Low/Medium/High):	Mitigation Measures:
Assessor Name:		
Date of Assessment:		
Next Review Date:		

16. Annex II: Internal Unusual Transaction Report

Internal Unusual Activity Report		
Date of report:		
Client ID:		
Date of account registration:		
Account status (Active/Suspended/Blocked):		
Risk rating:		
Account balance:		
Client details:	Client full name:	
	E-mail:	
	Phone number:	

	Brand registration:	
	Date of birth:	
	Nationality/Country of registration:	
	Address:	
	Due diligence documents held:	
Reason for reporting:		
Date of unusual activity/transaction:		
Attachments:		Records of CDD, Correspondence Records, Transaction Records
Provide details (e.g. dates and amounts) of any known intended or pending transactions:		

Name (reporting employee):	Signature:	Date:
----------------------------	------------	-------

17. Annex III: Geographical Risk Classification

<u>High-risk countries</u> <u>include but not limited</u> <u>to:</u>	- Philippines - Russia - Somalia - South Africa - South Sudan - Syria - Tanzania - Uganda - United Arab Emirates - Vanuatu - Venezuela - Vietnam - Yemen	- Singapore - Sint Maarten, Kingdom of the Netherlands - Suriname - Sweden - Turks and Caicos Islands
- Afghanistan - Algeria - Angola - Belarus - Bulgaria - Burkina Faso - Burma (Myanmar) - Cameroon - Central African Republic - China - Côte d'Ivoire - Croatia - Cuba - Democratic People's Republic of Korea - Democratic Republic of the Congo - Ethiopia - Gibraltar - Haiti - Iran - Iraq - Kenya - Lebanon - Libya - Mali - Monaco - Mozambique - Namibia - Nicaragua - Nigeria - Panama	<u>Low-risk countries include but not limited to:</u> - Antigua and Barbuda - Aruba, Kingdom of the Netherlands - Belize - Bermuda - Cayman Islands - Denmark - Dominica - Finland - Grenada - Guyana - Montserrat - New Zealand - Norway - Saint Kitts and Nevis - Saint Lucia - Saint Vincent & the Grenadines	<u>Excluded markets include, but not limited to:</u> - Aruba - Australia - Austria - Belgium - Bonaire - Czech Republic - Curaçao - France - Germany - Greece - Lithuania - Saba - Sint Eustatius - Spain - The Netherlands - United States of America