

Gameplay International B.V.

(Reg. 148409)

Customer Acceptance Policy

Approved by the Board of Directors



Effective Date: 02/09/2025

Next Review Date: September 2026

Dr. H. Fergusonweg 1, Willemstad, Curaçao

1. Policy Statement and Scope

Gameplay International B.V. has implemented this Customer Acceptance Policy to define clear standards, procedures, and requirements for approving customers on its online gaming and betting platform. The objective of the policy is to safeguard the company against being exploited for money laundering, terrorist or proliferation financing, sanctions evasion, fraud, or other forms of illicit activity. At the same time, it ensures full compliance with Curaçao's regulatory obligations, including the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (SNO), the Kingdom Sanction Act, and the National Ordinance on Games of Chance (LOK).

This policy has been designed in line with the guidance of the Curaçao Gaming Control Board and forms an integral part of Gameplay International B.V.'s broader Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) program. It also incorporates internationally recognised best practices, including the Financial Action Task Force (FATF) Recommendations and the European Union Anti-Money Laundering Directives.

The provisions of this policy apply to all directors, officers, employees, contractors, and third parties involved in onboarding and customer verification activities. Customers are not permitted to deposit, withdraw, or place wagers on the platform until they have satisfied all acceptance criteria and completed the full verification and screening process.

The scope of this policy extends to all individuals and entities seeking to open an account with Gameplay International B.V., irrespective of the registration channel. This includes direct sign-ups via the company's official website, mobile applications, affiliate networks, or third-party platforms. It governs the customer relationship from the point of application through to account closure or termination and applies to all products and services offered under Curaçao gaming licence OGL/2024/511/0630.

2. Compliance with Curaçao's Regulatory Framework

Gameplay International B.V. considers its Customer Acceptance Policy a central element of its broader framework for Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF). The policy is designed to operate in full compliance with Curaçao's legislation, including the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (SNO), the Kingdom Sanction Act, and the National Ordinance on Games of Chance (LOK).

Meeting these obligations is treated as a key operational priority. Customer acceptance processes are fully integrated into the company's compliance system so that due diligence is not limited to onboarding but continues throughout the entire business relationship. This ensures that any material changes in a customer's risk profile, behaviour, or jurisdiction are detected and addressed in a timely manner.

Employees who take part in onboarding or verification activities must complete specialised training that covers Curaçao's legislative framework and the company's internal compliance procedures. Training focuses on practical application of the Risk-Based Approach, recognition and escalation of high-risk indicators, and correct escalation procedures to the Compliance Officer or senior management.

In addition, Gameplay International B.V. engages independent auditors at least once per year to assess the effectiveness of the Risk-Based Approach and the implementation of this policy. These audits review processes such as identity verification, sanctions and PEP screening, Enhanced Due Diligence (EDD), and ongoing customer monitoring. Audit findings are formally presented to the Board of Directors, and any deficiencies are addressed promptly through corrective actions within defined timeframes, ensuring continuous compliance and operational integrity.

3. Customer Admission Criteria

Gameplay International B.V. accepts only those customers who meet all legal, regulatory, and internal compliance requirements. Before being granted access to the platform, each applicant must be verified to confirm that they have reached the minimum legal gambling age, which is eighteen (18) years or older if the laws of their jurisdiction set a higher threshold. Applicants must also provide accurate and verifiable details, including their full legal name, date and place of birth, nationality, and current residential address.

The company does not register customers who are based in, accessing services from, or conducting transactions within jurisdictions that fall under Curaçao's restrictions, international sanctions, or Gameplay International B.V.'s internal prohibited country list. As part of the verification process, all applicants are screened against sanctions lists issued by bodies such as the United Nations, the European Union, the U.S. Office of Foreign Assets Control (OFAC), the U.K. Office of Financial Sanctions Implementation (OFSI), the Sanctions National Ordinance, the Kingdom Sanction Act, and any applicable lists published by the Curaçao Gaming Control Board.

All funds used for betting or gaming must originate from legitimate and lawful sources. Where a customer's profile indicates heightened risk, additional documentation may be required to verify both the source of funds and, where relevant, the source of wealth. Gameplay International B.V. also reserves the right to refuse services to individuals or entities with a documented history of fraud, chargebacks, bonus abuse, breaches of gambling rules, or those who have previously self-excluded due to problem gambling.

4. Applying the Risk-Based Approach

Gameplay International B.V. follows a structured Risk-Based Approach (RBA) both during customer onboarding and throughout the lifecycle of the relationship. This ensures that the depth of due diligence applied is proportionate to the level of risk associated with each customer.

The assessment process evaluates a range of factors, including the customer's personal and financial background, the types of products and services they intend to use, potential

geographic risks, and vulnerabilities linked to the technology or channels through which services are accessed. By considering these elements together, the company ensures that higher-risk situations are subject to stronger controls while lower-risk relationships are managed under standard due diligence procedures.

4.1 Customer Risk Profile Assessment

Gameplay International B.V. evaluates every applicant to determine their potential exposure to money laundering, terrorist financing, or proliferation financing risks. This process ensures that the level of due diligence applied is proportionate to the customer's specific risk profile.

Risk Level	Typical Characteristics	Due Diligence Measures
Low Risk	Clear and verifiable source of income; stable employment in low-risk sectors; gambling and transactions consistent with declared profile.	Standard Customer Due Diligence (CDD).
Medium Risk	Legitimate income that is harder to verify; employment in moderately exposed sectors; occasional inconsistencies in transactional behaviour.	Standard CDD with extra verification steps and closer monitoring.
High Risk	Multiple or unclear income sources; work in high-risk industries (e.g., cryptocurrency, unregulated finance); activity inconsistent with stated income; Politically Exposed Persons (PEPs) and their associates.	Enhanced Due Diligence (EDD), senior management approval, continuous monitoring, and additional documentation requirements.

Indicators triggering enhanced scrutiny

- Customers with several income sources must provide supporting evidence for each, such as payslips, tax filings, business accounts, or investment records. Where income is irregular or inconsistent, for example seasonal or commission-based, documentation must prove the lawful origin of funds, with ongoing monitoring applied to detect unusual behaviour.
- PEPs and their close associates are always treated as high risk and require comprehensive checks on source of wealth and funds, senior management approval prior to activation, and continuous monitoring.

- Customers placing unusually large or frequent wagers must demonstrate legitimate fund origins through bank statements or other verifiable records.
- Spending that is disproportionate to declared income requires further justification with additional documents.
- Sudden unexplained increases in betting activity, especially among casual or tourist players, trigger reclassification and enhanced monitoring.
- Use of third parties to deposit, withdraw, or gamble on behalf of a customer is flagged for investigation, with all parties subject to verification.
- Attempts to operate multiple accounts are treated as suspicious, with linked accounts consolidated and reviewed in detail.
- Requests to redeem large volumes of chips without linked verifiable activity require full identity and source-of-funds checks before processing.
- Customers connected to junket operators are automatically deemed high risk, with EDD applied to both the customer and the operator, including full review of financial arrangements and funding sources.

Ongoing monitoring

Gameplay International B.V. continuously monitors customer activity to ensure that risk profiles remain accurate. Reviews are carried out on a risk-based schedule and triggered by material changes, such as unusual transaction patterns, unexplained large deposits, or updated personal or financial details. If a customer's risk level increases, the company applies stronger controls, including EDD, closer transaction monitoring, or restrictions on account activity. This ensures that risk management remains dynamic, effective, and compliant with regulatory standards.

4.2 Risks Connected to Products, Services, and Transactions

The overall risk profile of a customer is influenced not only by their personal circumstances but also by the products, services, and transaction types they engage with. Certain activities present higher risks due to limited transparency or traceability. These include peer-to-peer transfers, the purchase or exchange of gaming tokens, or the use of anonymous or semi-anonymous funding methods such as prepaid cards or certain cryptocurrencies.

Accounts that appear to function mainly as financial conduits rather than for genuine gameplay—for example, large deposits followed by minimal betting before withdrawal—are subject to closer examination. The same applies when payment methods not registered to the account holder are used, as these are considered red flags and require additional verification.

Gameplay International B.V. monitors and addresses several critical risks in this area:

Risk Factor	Example Behaviour	Mitigation Measures
Funds of criminal origin	Deposits linked to fraud, narcotics trafficking, or theft	Request proof of legitimate funds; report suspicious cases to FIU
Anonymous payment methods	Use of prepaid cards, certain cryptocurrencies, or virtual assets	Apply enhanced verification; require documented source of funds
Improper account use	Large deposits, little or no gameplay, followed by withdrawals	Immediate review and possible suspension pending investigation
Third-party payments	Account funded via payment method not registered to customer	Verify both parties; establish relationship; confirm fund legitimacy
Transfers between accounts	Customer-to-customer transfers	Generally prohibited; exceptions require Compliance Officer approval
Multiple accounts or wallets	Operating several accounts across company platforms	Detect and link accounts via internal monitoring; consolidated review
Frequent payment method changes	Regularly switching bank accounts or e-wallets	Trigger profile review; apply Enhanced Due Diligence if needed
Identity fraud	Use of stolen personal or banking details to fund accounts	Apply robust KYC and document authenticity checks; report suspected fraud
Electronic wallets	Use of wallets from weakly regulated jurisdictions or with anonymous deposits	Verify source of funds; confirm provider licensing and regulatory standards

4.3 Geographic Risk Considerations

Gameplay International B.V. maintains a geographic risk assessment framework to evaluate potential risks associated with a customer's country of residence and the origin of their funds. This framework is regularly updated based on trusted international sources, including public statements from the Financial Action Task Force (FATF), advisories from the Caribbean Financial Action Task Force (CFATF), the European Commission's list of high-risk third countries, the U.S. Office of Foreign Assets Control (OFAC) sanctions lists, the U.S. Department of State's International Narcotics Control Strategy Reports, and Transparency International's Corruption Perceptions Index.

Customers from sanctioned jurisdictions are automatically refused, while applicants from high-risk jurisdictions may only be onboarded after completing Enhanced Due Diligence (EDD), subject to approval by senior compliance staff.

A jurisdiction is classified as high risk where one or more of the following conditions apply:

- Countries with weak or poorly enforced AML/CFT systems. Customers from these jurisdictions must provide comprehensive documentation regarding their source of funds and wealth, and their activity is monitored continuously.
- Countries with systemic corruption, which heightens the risk of illicit funds entering the gaming system. Customers from such countries face stricter verification, with particular emphasis on income legitimacy.
- Countries under international sanctions relating to terrorism, weapons proliferation, or other criminal activities. These customers are generally prohibited, although exceptional cases may be considered if senior management grants explicit approval and full EDD is applied.
- Countries linked to active terrorist organisations, where customers must undergo enhanced verification, intensive monitoring, and frequent transaction reviews.

To ensure accuracy, Gameplay International B.V. consults authoritative lists and reports, including FATF high-risk and monitored jurisdictions, CFATF public statements, European Commission AML/CFT deficiency lists, OFAC sanctions, U.S. State Department reports, and Transparency International's indices. Reports identifying countries supporting terrorist financing or harbouring terrorist organisations are also reviewed.

If a customer's residence or source of funds appears on a high-risk or sanctioned list, the application is escalated to the Compliance Officer for review. Should onboarding proceed, EDD measures are mandatory. These include thorough identity verification, detailed examination of source of funds and wealth, and enhanced transaction monitoring throughout the customer relationship.

4.4 Risks Associated with Channels and Technology

The methods customers use to access Gameplay International B.V.'s platform and the technologies involved have a direct impact on their risk profile. Remote onboarding in particular carries elevated risks of impersonation and identity fraud. To mitigate these risks, the company uses advanced digital Know Your Customer (KYC) solutions, including

biometric verification, document authenticity checks, geolocation confirmation, and multi-factor authentication.

Before introducing new technologies, payment methods, or platform features, Gameplay International B.V. conducts a thorough pre-launch risk assessment to ensure they cannot be exploited for money laundering, fraud, or other illicit activity.

Certain channels and practices are treated with greater caution. Any access point that allows a customer to remain anonymous is classified as high risk. In these cases, enhanced identification and verification measures are enforced, including biometric validation, document checks, and real-time screening against sanctions and Politically Exposed Person (PEP) databases. While remote interaction has become standard across the industry, it still requires strong safeguards to prevent misuse. For this reason, the company applies secure verification processes such as biometric checks, liveness detection, and automated document validation during onboarding and subsequent transactions.

Additional risk arises when third parties are involved in customer interactions, particularly when the intermediary is not subject to its own AML/CFT obligations. In such cases, Gameplay International B.V. performs due diligence on both the customer and the intermediary. This includes confirming the third party's regulatory status, evaluating the strength of its AML/CFT controls, and verifying that the information provided is accurate and complete.

4.5 Risk Indicators

Gameplay International B.V. uses a structured set of risk indicators to evaluate the overall risk profile of each customer. These indicators are integral to the company's Risk-Based Approach (RBA) and ensure that the level of due diligence applied reflects the specific risks identified.

The first category relates to the customer's personal and financial profile. Risk indicators in this area include multiple or inconsistent sources of income, designation as a Politically Exposed Person (PEP) or close associate, patterns of excessive or disproportionate spending, sudden increases in activity among casual or tourist players, the use of third parties to transact, the operation of multiple accounts, attempts to redeem chips without linked verifiable gameplay, or connections to junket operators.

The second category concerns products, services, and transactional behaviour. Red flags here include evidence of criminal proceeds, reliance on anonymous or unregulated payment methods, improper use of gaming accounts, frequent use of third-party funding, repeated changes in payment methods, use of prepaid cards or multiple e-wallets, and identity fraud.

The third category is linked to geographic risk. Higher risk applies to customers from jurisdictions with weak AML/CFT frameworks, high levels of corruption, active sanctions, or known links to terrorism. Jurisdictions highlighted by bodies such as FATF, CFATF, OFAC, or Transparency International's Corruption Perceptions Index are also classified as elevated risk.

The fourth category relates to channels and technology. Increased risk is associated with customers who register or transact through channels that allow anonymity, use remote onboarding without sufficient safeguards, or rely on unregulated third-party intermediaries.

Outcome of the Risk Assessment

The final risk classification assigned to a customer dictates the level of due diligence to be applied. Customers assessed as low risk are managed under standard monitoring and verification procedures. By contrast, customers identified as high risk must undergo Enhanced Due Diligence (EDD), which involves additional verification measures, senior management approval prior to onboarding, and continuous enhanced monitoring. These customers are subject to stricter oversight throughout the relationship to ensure that any unusual or suspicious behaviour is promptly detected and addressed.

5. Customer Onboarding Process

Gameplay International B.V. follows a structured, compliance-driven onboarding procedure to ensure that only customers who meet the company's acceptance standards are granted access to its platform. No account is activated until the applicant has successfully completed all required stages of identification, verification, and sanctions screening.

Identification Requirements

At the point of registration, customers must provide key personal details, including their full legal name, date and place of birth, nationality, current residential address, and an official identification number such as a passport or national identity card.

Sanctions and PEP Screening

All applicants are screened against international sanctions registers and Politically Exposed Person (PEP) databases using automated screening tools for wide coverage. Any matches or alerts generated are manually reviewed by trained compliance officers to confirm accuracy and eliminate false positives before proceeding.

Enhanced Verification for High-Risk Customers

Where the initial assessment identifies a customer as high risk, further verification steps are applied. In such cases, customers are required to provide evidence of the legitimacy of their funds and, if applicable, their source of wealth. Acceptable documents may include recent bank statements, audited business records, tax filings, property sale agreements, or investment account statements. These enhanced procedures ensure that high-risk applicants are reviewed thoroughly, in line with both regulatory obligations and the company's internal standards, thereby protecting the platform from misuse.

6. Enhanced Due Diligence

Enhanced Due Diligence (EDD) is applied to customers who present a heightened risk profile. This category includes Politically Exposed Persons (PEPs), their close associates and family members, customers residing in or funding accounts from high-risk jurisdictions, individuals conducting unusually large, complex, or unexplained transactions, and those whose financial activity does not correspond with their declared income or business profile.

Measures and Verification

EDD requires a more thorough level of scrutiny than standard due diligence. The process involves a detailed review of both the customer's source of funds and source of wealth, supported by credible, independent documentation. Where relevant, this may include corporate registry searches, confirmation of beneficial ownership, verification of employment or business ownership, assessment of audited financial statements, and extensive adverse media and reputational checks from multiple sources.

Approval and Oversight

All high-risk customers must be approved by senior management before onboarding can proceed. In particularly sensitive or complex cases, formal approval may also be required from the Board of Directors.

Monitoring after Onboarding

Customers classified as high risk remain subject to heightened oversight once accepted. This includes stricter thresholds for transaction reviews, closer scrutiny of activity patterns, and more frequent risk profile reassessments. These measures ensure that high-risk relationships are controlled in a responsible manner, consistent with regulatory requirements and the company's internal risk tolerance.

7. Ongoing Monitoring

Gameplay International B.V. recognises that customer acceptance is not a one-time exercise but an ongoing responsibility. Continuous monitoring ensures that customer activity remains consistent with the risk profile established at registration and that any irregular or suspicious behaviour is promptly identified and addressed.

Automated Transaction Monitoring

The company employs automated systems designed to detect unusual or high-risk activity. Alerts are triggered for patterns such as deposits or withdrawals inconsistent with the customer's profile, rapid fund movement without meaningful gameplay, use of multiple or unusual payment methods, or behaviours suggestive of collusion, chip-dumping, or other prohibited practices. Each alert is reviewed by compliance officers, who evaluate the context and determine whether escalation or further investigation is necessary.

Periodic Reviews and Risk Re-Evaluation

In addition to real-time monitoring, Gameplay International B.V. conducts periodic reviews of customer profiles on a risk-based schedule. These reviews ensure that classifications remain current and accurate. Material changes—such as relocation to a high-risk jurisdiction, significant increases in transaction volumes, or changes in funding methods—prompt immediate reassessment of the customer's risk level. Where required, enhanced monitoring or additional safeguards are applied to manage emerging risks effectively.

8. Termination of Customer Relationships

Gameplay International B.V. reserves the right to suspend or terminate a customer relationship whenever required by law, internal compliance policies, or risk considerations. Termination may occur if a customer fails to provide the required identification or supporting documents within thirty calendar days, if activity gives rise to reasonable suspicion of money laundering, terrorist financing, or proliferation financing, or if the customer engages in behaviour that breaches applicable laws, regulations, or the company's Responsible Gambling Policy.

Handling of Funds and Reporting

If the termination is linked to suspected criminal activity, Gameplay International B.V. promptly files a report with the Financial Intelligence Unit (FIU) in line with the National Ordinance on the Reporting of Unusual Transactions (NORUT). Any remaining account balance is returned to the original funding source, unless there is a legal requirement to freeze or seize funds pending investigation. Detailed records of all terminations, including the reasons and supporting documentation, are maintained for a minimum of five years.

Circumstances Leading to Refusal or Termination

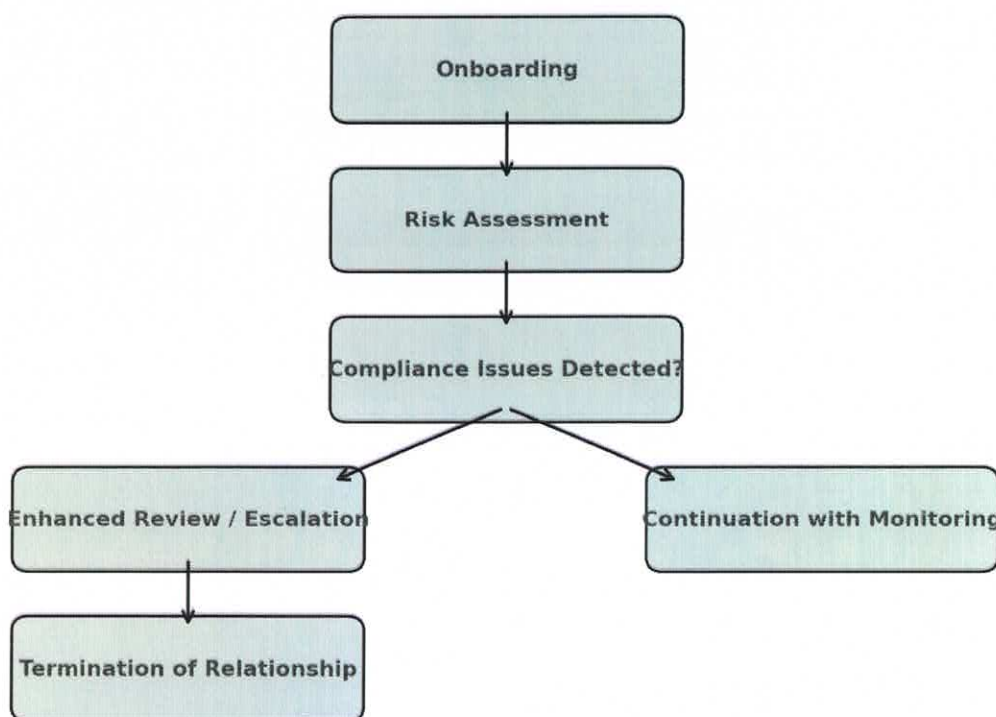
The company will decline onboarding or terminate service where customers:

- Reside in, access services from, or transact through prohibited or sanctioned jurisdictions.
- Fail to provide requested documentation or information within the specified timeframe.
- Submit false, misleading, or incomplete details during registration or verification.
- Cannot demonstrate that their funds or wealth are from legitimate sources.

- Are involved in, or suspected of, money laundering, terrorist financing, or other criminal activities.
- Are Politically Exposed Persons (PEPs) whose risks cannot be effectively mitigated.
- Engage in fraudulent conduct, bonus abuse, collusion, or other prohibited gambling activities.
- Attempt to use third parties to transact without proper disclosure and verification.
- Have self-excluded or been excluded for responsible gambling concerns.
- Redeem large amounts of chips or request withdrawals without verifiable related gaming activity.

- Are minors or otherwise below the legal gambling age in their jurisdiction.

Termination Decision Flow - Gameplay International B.V.



9. Integration with Responsible Gambling

Gameplay International B.V. ensures that its Customer Acceptance Policy is closely aligned with the company's Responsible Gambling framework. Protecting customers from gambling-related harm is treated as a fundamental part of the compliance and operational system.

Indicators of Gambling-Related Harm

When a customer displays behaviour suggesting potential harm—such as frequent deposits that appear to exceed their financial capacity or excessively long gaming sessions—the company may intervene. Actions can include setting deposit or wagering limits, temporarily suspending the account, or, if necessary, refusing further service to protect the customer.

Self-Exclusion and Account Controls

Requests for self-exclusion are implemented without delay and applied across all accounts linked to the customer to prevent circumvention. These restrictions remain active for the period requested by the customer or for as long as required under applicable regulations.

Staff Training and Awareness

All employees in customer-facing roles receive targeted training to help them identify early signs of problem gambling. This training is integrated into both the onboarding process and ongoing monitoring so that intervention is timely whenever potential risks emerge.

10. Record Keeping

Gameplay International B.V. maintains complete and detailed records relating to customer acceptance for at least five years following the end of a business relationship, in accordance with regulatory requirements. These records include identification and verification documents, proof of address, evidence of the source of funds and wealth, transaction monitoring alerts, investigation reports, Enhanced Due Diligence (EDD) files, internal compliance assessments, and documentation concerning account suspensions or terminations.

All records are securely stored in encrypted form, with strict access controls to protect confidentiality and data security. Access is granted only to authorised staff, and all access activities are logged and periodically reviewed to ensure compliance with data protection standards and internal policies.

11. Policy Review and Approval

This Customer Acceptance Policy is reviewed at least once every twelve months to confirm its ongoing effectiveness and compliance with legislation, regulatory expectations, and industry best practices. The review process also evaluates changes to the company's risk profile, customer behaviour trends, and technological developments that may introduce new vulnerabilities.

Any proposed amendments are drafted by the Compliance Officer and submitted to the Board of Directors for approval before being implemented. All updates are documented in full, and staff are informed and trained to ensure consistent application of the revised policy across the organisation.