

CUSTOMER ACCEPTANCE POLICY (CAP)

**BRIGHTSTAR N.V.
Kaya W.F.G., (Jombi) Mensing 24,
Unit A,
Willemstad | Curaçao**

Last Updated 08.05.2025

I. Introduction

1. Purpose

The Customer Acceptance Policy (CAP) is designed to establish comprehensive guidelines and procedures for the acceptance of customers, ensuring compliance with all relevant legal, regulatory, and internal standards. This policy aims to protect the integrity of our operations, promote responsible gambling, and maintain a secure environment for both our customers and staff.

2. Scope

This policy applies to all new and existing customers of Brightstar N.V., encompassing all areas of customer interaction including registration, gaming activities, financial transactions, and customer support services. It is mandatory for all employees, contractors, and stakeholders involved in customer interactions to adhere to the provisions of this policy. Additionally, this policy includes clear and fair criteria and procedures for account termination, whether initiated by the customer or the company.

3. Objectives

The primary objectives of this Customer Acceptance Policy are as follows:

- Ensure that Brightstar N.V. operates within the legal framework and adheres to all regulatory requirements.
- Promote responsible gambling practices and provide support for problem gambling.
- Prevent money laundering and other illicit activities through rigorous customer verification and monitoring.
- Create and maintain a safe, enjoyable, and respectful environment for all customers and staff.

4. Commitment to Compliance and Integrity

Brightstar N.V. is committed to maintaining the highest standards of compliance and integrity in all its operations. This policy is an integral part of our commitment to uphold these standards and ensure that our customer acceptance processes are robust, transparent, and fair.

5. Policy Review and Updates

The Customer Acceptance Policy is subject to regular review and updates to ensure it remains effective and aligned with evolving legal, regulatory, and business requirements. The management team, in collaboration with the Compliance Officer, will conduct these reviews and implement necessary amendments to continuously improve our customer acceptance practices.

II. Customer Registration Phase

1. Player Identification

Player identification is the collection of personal details of the player to establish their identity. At minimum, Brightstar N.V. collects the following information immediately upon registration:

- Full name;
- Permanent residential address;
- Date of birth;
- Gender;
- Phone number;
- Email address.

During the registration phase, Brightstar N.V. ensures the person registering the personal details is the beneficial owner of the account, and the account is to be used entirely for recreational purposes. Email verification is immediately requested after submitting the sign-up request.

Brightstar N.V. initiates the AML verification process from the point of registration. Upon registration, an immediate automated initial PEP/Sanction/Adverse Media screening is performed using NOTO – 360 Fraud and Compliance. Any positive result is flagged, and the individual will not be allowed to engage in any gaming or financial activities until cleared through a comprehensive investigation by the dedicated departments (Risk/Fraud/AML & DD).

2. PEP / Sanction screening

The regulatory requirement for screening Politically Exposed Persons (PEPs) and individuals on sanction lists is a critical component of anti-money laundering (AML) and counter-terrorism financing (CTF) frameworks. This practice is essential for mitigating risks associated with financial crimes, corruption, and illicit activities.

Financial institutions and casinos are mandated to identify and monitor PEPs to prevent the misuse of the financial system. Enhanced Due Diligence (EDD) measures, such as thorough background checks and ongoing monitoring of financial transactions, are required.

Sanction lists are compiled by governments and international bodies (e.g., United Nations, European Union, OFAC) and include individuals, entities, and countries subject to economic and trade restrictions. Organizations must screen customers against these lists to ensure they do not engage in prohibited transactions. This involves initial screening during customer onboarding and continuous monitoring to detect any changes in status.

Therefore, for Brightstar N.V. to be fully compliant with the international regulatory standards, it performs an automated initial PEP / Sanction screening on every individual during the registration phase provided by *NOTO - 360 Fraud and Compliance*. Any positive result is flagged and the individual is not allowed to engage in any activities until a comprehensive investigation has been performed by the dedicated teams (Risk/Fraud/AML & DD). Sanctioned individuals are subject to account freezing and external reporting to the FIU, and PEP matches are subject to further Enhanced Due Diligence (EDD) measures and ongoing monitoring.

III. Customer Risk Assessment

1. Threshold Approach

Customers of Brightstar N.V. are permitted to engage in gaming & financial activities only after they have been adequately identified, screened, and verified, and after the nature of the business relationship has been established, which must be solely for the purpose of gaming.

Brightstar N.V. applies a threshold-based risk management approach to customer activities. Automatic reporting detects and lists all accounts passing specific thresholds within the past 24 hours. Each new threshold prompts a review by the dedicated departments to establish a customer risk profile and ensure the customer's activity remains aligned with their established profile.

Three existing levels of residual player risk exist: Low (Green), Medium (Amber), and High (Red). Further details on the risk-based approach and risk levels are provided in Brightstar N.V.'s Business Risk Assessment and KYC, AML & CTF Policy.

The first AML threshold for full Customer Due Diligence (CDD) measures is set at EUR 2,000 cumulative transaction activity (lifetime). Customers who have registered and have not yet reached this EUR 2,000 cumulative transaction threshold are automatically classified as low risk, provided no sanctions, PEP, or adverse media flags have appeared at registration or subsequently.

2. The AML Deposit Thresholds

2.1. Initial AML Deposit Threshold – EUR 2,000 lifetime (LT) deposits

This threshold integrates the customer fully into Brightstar N.V.'s AML workflow. Although verification begins at registration, additional verification measures become mandatory at this point.

At this EUR 2,000 cumulative transaction threshold, the customer is required to provide:

- A valid government-issued identity document (passport, national ID, or driver's license);
- A proof of address (utility bill or bank statement dated within the past six months);
- Copies of the cards or e-wallets used for deposits.

This EUR 2,000 threshold is calculated daily, including all deposits, withdrawals, and peer-to-peer transfers.

Brightstar N.V. also conducts another PEP/Sanction/Adverse Media screening using Refinitiv World Check at this threshold, ensuring continued low-risk exposure. Once the EUR 2,000 threshold is reached:

- A formal customer risk assessment is conducted;
- Full CDD measures are applied according to the customer's risk level;
- Enhanced Due Diligence (EDD) is carried out if increased risks are identified.

If the threshold is triggered due to a deposit, the customer will not be permitted further deposits or withdrawals until verification is fully completed, but may continue to use their existing account balance for gaming.

If triggered by a withdrawal request, the customer's account will be restricted from further transactions until verification is successfully completed.

After this threshold, should indications of money laundering arise, we also consider filing a Suspicious Activity Report (SAR), irrespective of the payment method used.

2.1.1. Transaction Limits – Deposits and Withdrawals

Brightstar N.V. adheres to specific limits per transaction and per daily activity to mitigate AML risks effectively. These transaction limits are strictly enforced alongside cumulative lifetime thresholds and ongoing customer verification.

- **Deposit Limits:**

Brightstar N.V. **does not accept deposits exceeding EUR 2,000 per single transaction.** Any attempt to exceed this limit will be declined, and repeated attempts may trigger additional verification checks.

- **Withdrawal Limits:**

Brightstar N.V. **does not process withdrawals exceeding EUR 2,000 within a single calendar day.** Customers requesting withdrawals above this daily limit will be required to split transactions across multiple days, and additional due diligence measures may be initiated based on the customer's profile and transaction patterns. These per-transaction and daily withdrawal limits operate concurrently with lifetime thresholds and ongoing AML monitoring procedures. They complement the company's efforts to identify and respond to unusual or potentially suspicious transactions promptly.

2.1.2. Failure to Complete Checks (AML Threshold – EUR 2,000)

If a customer does not provide the required information or documentation to complete the CDD or EDD process, Brightstar N.V. will not process further transactions with or for the customer through any payment methods.

While the verification process is ongoing:

- If the EUR 2,000 threshold is met due to a deposit, the customer will not be able to deposit or withdraw additional funds but may continue gaming with their existing balance.
- If the EUR 2,000 threshold is met due to a withdrawal request, the account will be restricted, preventing any further transactions until verification is completed.

If the customer fails to submit the required documentation within 30 days of reaching the EUR 2,000 threshold, Brightstar N.V. will:

- Restrict or terminate the business relationship with the customer;

- Report the transaction to the Financial Intelligence Unit (FIU) if suspicion of money laundering or terrorist financing exists;
- If no suspicion of financial crime exists, funds will be returned to the original deposit source.

Internal procedures will govern the decision-making process in situations involving suspicion of money laundering or terrorist financing, with careful consideration given to the risk of “tipping off” the customer.

2.2. 10K to 100K LT AML Deposit Thresholds

Players who are allowed to continue after a successful identity verification and making sure they do not present an increased risk to Brightstar N.V. are subject to ongoing transactional & gaming activity monitoring. This monitoring occurs at every EUR 10,000 deposits between 10K lifetime and 100K lifetime. This ensures that unusual transactions or patterns of transactions are identified and reviewed, and that the client stays consistent with the established background and risk profile.

- At every new threshold reached, an extensive review is performed by the respective departments which consists of new World Check screenings, background searches on the public space and full transactional and gaming activity reviews. A risk-based approach is applied after each review to determine the current player risk and to dictate if any measures should be taken. A risk category may change from low to high or vice versa depending on new emerging risks and other factors. Players may be placed on a periodic monitoring if it is deemed necessary.

Source of Funds and Source of Wealth (SoF/SoW) information and documentation can be requested from the client at any point in time if the AML department requires it. Usually, it is done at the higher deposit thresholds and depending on the activity, but if/when a client reaches the final threshold of EUR 100K lifetime deposits and by that time we do not have satisfactory SoF/SoW documentation or direct information from the customer submitted at an earlier stage, the SoF/SoW process will be initiated by the AML department and we'll either ask for answers to the SoF/SoW questionnaire alone or for answers along with documents.

2.3. Above the 100K LT Deposit Threshold

Customers who continue to use Brightstar N.V.'s services after passing the 100K (EUR) LT deposit threshold are not relieved from ongoing monitoring and periodic screening.

Players at this level have displayed satisfactory data about their SoF/SoW profiles and their activity corresponds with it. As they've passed the automated thresholds, they're all now subject to manual ongoing monitoring done by the AML department.

The ongoing monitoring period may vary depending on the risk category. Players presenting an increased risk to Brightstar N.V. will be placed on a shorter monitoring period (e.g. weekly/biweekly/monthly), and those players who are of standard/lower risk will be monitored on a longer period (e.g. 2-month, 3-month, etc.).

3. Player Profile Updates

The background & employment profile of a customer may change with time. To ensure that Brightstar N.V. has up-to-date information about its players, at certain periods of time during ongoing monitoring, the clients will be reviewed for potential changes of their background & employment profiles based on information available publicly or derived from previously provided documentation (e.g. employment contract with an end of term date). The unavailability of such information may prompt Brightstar N.V. to request up-to-date SoF/SoW data directly from the client.

At every ongoing monitoring review, players are screened for PEP / Sanctions lists and checked for any new adverse media appearances.

Risk categories and monitoring periods can be changed at any time should concerns arise. Further SoF/SoW and other measures can be taken at any time, regardless of the amount of documentation & information we have on a client if their behavior becomes inconsistent with the established profile.

4. Account Termination

Brightstar N.V. terminates existing accounts and ends customer relationships under the following circumstances:

- **Sanctions Lists:** If it is discovered that a customer may be linked to a sanctions list. These lists are compiled by various national and international bodies, including but not limited to:
 - The United Nations (UN)
 - The European Union (EU)
 - The United States Department of the Treasury's Office of Foreign Assets Control (OFAC)
 - The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

- Her Majesty's Treasury (HMT) in the United Kingdom

Sanctions lists include individuals, entities, and countries subject to economic and trade restrictions aimed at preventing activities such as terrorism, the proliferation of weapons of mass destruction, human rights abuses, and other illicit activities.

- **CDD Process:** If the full Customer Due Diligence (CDD) process, including the complete identification and verification of player data, **is not completed within the allowed 30-day period after reaching the EUR 2,000 cumulative transaction threshold.**
- **Suspicion of ML/TF:** If there are suspicions of money laundering (ML), terrorist financing (TF), or other significant compliance red flags.
- **Non-compliance with EDD:**

Brightstar N.V. applies Enhanced Due Diligence measures when a customer presents a higher-than-usual risk based on specific regulatory triggers or internal risk assessments. EDD may be initiated in the following circumstances:

- The customer is identified as a Politically Exposed Person (PEP);
- The customer resides in, or has ties to, a jurisdiction listed on the **FATF Grey List or Black List** (high-risk jurisdictions);
- There is suspicion of **fraud, misuse of identity**, third-party card use, or other **financial crime risks**;
- The customer demonstrates **unusually high spending patterns** or inconsistent activity relative to their profile;
- There are adverse media hits or suspicious background information.

The EDD process may include:

- Conducting extensive background checks using both public and commercial databases;
- Screening for adverse media, criminal records, and sanctions;
- Requesting **advanced verification documents** such as:
 - Source of Funds (SoF) documentation (e.g., bank statements, payslips, tax returns);
 - Source of Wealth (SoW) documentation (e.g., property sale contracts, inheritance records);
 - Employment or self-employment evidence (e.g., employment contract, company ownership records);

- Use of **third-party verification tools**, including credit reports, business registry extracts, and wealth/acuity reports.

If the customer fails to cooperate with EDD measures, or if the information provided is insufficient or unverifiable, Brightstar N.V. may restrict or terminate the customer relationship. These actions are also considered in the broader AML compliance framework and may involve reporting to the relevant authorities.

In addition to account termination, consideration will be given to reporting suspicious activities externally to the Financial Intelligence Unit (FIU).

Brightstar N.V. also monitors for other suspicious activities and transactions. If suspicions arise, the account remains active until the investigation concludes, to avoid tipping off the customer. All accounts and suspicious cases are handled in accordance with regulatory standards.

5. Recordkeeping

All records obtained through CDD/EDD measures, account files and business correspondence are kept for at least five (5) years after a business relationship ends. An account file is created at the threshold of 10K (EUR) LT deposits and is constantly updated with information from searches, reviews, correspondences and with decisions taken.

Various trackers have been created that are updated manually by the AML department. Player accounts are entered inside the trackers at every threshold that they reach, starting from 2K LT and after performing a review. The trackers contain information such as the relevant threshold, date of reaching it, risk level, actions taken, etc. Ongoing monitoring trackers are also available for accounts above the last threshold (100K LT) which help to track each player's financial activities, monitoring updates and risk level.

All of this enables Brightstar N.V. to comply with information requests from the competent authorities if such are requested as evidence for prosecution of criminal activity.



Starkeast Management B.V., Managing Director
Signed by: Menno Jordean, Managing Director
Date: May 9, 2025