

**KNOW YOUR CLIENT (KYC) ANTI-MONEY LAUNDERING (AML)
COUNTER TERRORIST FINANCING POLICY (CTF) & COMBATING
OF FINANCING OF PROLIFERATION (CFP)**

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

Version	Date	Description	Signed off
1.0	20.02.2024	Policy implementation	Nwankwo Chibuike Chinonso Justice (MLRO)
1.1	01.09.2024	Changes to policy in accordance with new Curacao regulations.	Nwankwo Chibuike Chinonso Justice (MLRO)
2.0	13.03.2025	Changes to policy in accordance with LOK and additional Curacao regulations.	Nwankwo Chibuike Chinonso Justice (MLRO)
2.1	14.04.2025	Revision of current policy based on specific guidelines by the CGA and full adaptation to LOK.	Nwankwo Chibuike Chinonso Justice (MLRO)

Policy History

Version 1.0 of this document represented the original implementation of Brightstar N.V.'s Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Combating Financing of Proliferation (CFP) policy. Subsequent versions reflect updates and refinements made to ensure continued alignment with evolving regulatory requirements, including guidance issued by the Curaçao Gaming Control Board (GCB) / Curaçao Gaming Authority (CGA).

Policy Statement

Brightstar N.V. is fully committed to preventing its operations from being used for money laundering, terrorist financing, or the financing of the proliferation of weapons of mass destruction. This Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Combating Financing of Proliferation (CFP) Policy outlines the Company's responsibilities and procedures in accordance with the legal and regulatory requirements of Curaçao and international best practices.

This policy applies to all employees, departments, third-party partners, and customers of Brightstar N.V. It forms part of the Company's broader risk management and compliance framework and is designed to ensure that effective internal controls are in place to detect, deter, and report suspicious activities.

Brightstar N.V. promotes a culture of compliance, transparency, and integrity across all business units and expects all individuals subject to this policy to adhere strictly to its principles and procedures.

1.0 INTRODUCTION AND LEGAL FRAMEWORK

The aim of this document is to define the policies, procedures, systems, and controls necessary to ensure that Brightstar N.V. ("Brightstar" or "the Company"), operating from Curaçao, meets its legal and regulatory obligations to prevent and combat money laundering, terrorist financing, and the proliferation of weapons of mass destruction. The Company is committed to compliance with the National Ordinance on Identification when Rendering Services (NOIS) and the National Ordinance on the Reporting of Unusual Transactions (NORUT), as well as additional regulations applicable to the gaming sector in Curaçao.

With the publication of the National Decree Supervisor Identification when Rendering Services (Gaming Sector) and the National Decree Supervisor Unusual Transactions (Gaming), the Curaçao Gaming Control Board (GCB) has been designated as the supervisory authority for AML/CTF/CFP compliance within the gaming sector. Brightstar N.V. aligns its policies and procedures with the guidance issued by the GCB to ensure full regulatory adherence.

The Company's approach to mitigating the risks of money laundering and terrorist financing includes the implementation of the following key procedures:

- Customer Identification and Verification (Know Your Client - KYC)
- Transaction Monitoring and Record Keeping
- Staff Training and Development
- Internal Reporting of Suspicious Transactions
- Cooperation with Regulatory and Law Enforcement Authorities

Brightstar N.V. will not engage in business relationships with individuals or entities where there is a reasonable suspicion of involvement in illicit activities. If suspicions arise regarding a participant's involvement in illegal activities, the Company will act in accordance with its internal procedures, including reporting the matter to the Curaçao Financial Intelligence Unit (FIU) and, if necessary, terminating the relationship in collaboration with relevant authorities to prevent any breach of "tipping-off" provisions.

1.1 APPLICABLE LAWS AND REGULATIONS

The Company's AML/CFT/CFP policies are based upon the following laws, regulations, and guidance issued by the Curaçao Gaming Control Board:

- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92)
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99)
- Ministerial Decree with General Operation of November 11, 2015, laying down the indicators for unusual transactions (N.G. 2015, no. 73)
- Sanctions National Ordinance (N.G. 2014, no. 55)
- Kingdom Sanctions Act (N.G. 2016, no. 54)
- National Decree Entering into Force of Kingdom Sanctions Law (N.G. 2017, no. 2)
- National Decree Implementing United Nations' Security Council Resolutions on Sanctions (N.G. 2015, no. 28, 29, 30)
- National Ordinance Extension of Validity of Sanction Decrees 2018 (N.G. 2018, no. 34)
- The Penal Code of Curaçao (N.G. 2011, no. 48)

These laws and regulations form the legal basis for combating money laundering, terrorist financing, and the proliferation of weapons of mass destruction within the Curaçao gaming sector. Brightstar N.V. is fully committed to compliance with these regulations and to upholding the highest standards of integrity and transparency in all its operations.

1.2 AUDIENCE

This policy applies to all individuals and entities that have a role or responsibility in upholding Brightstar N.V.'s compliance with Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Combating Financing of Proliferation (CFP) obligations. The following stakeholders are specifically covered by this policy:

- **All Employees:** Including permanent, temporary, part-time, and contract staff engaged in any capacity across departments such as Operations, Customer Support, Finance, Compliance, and IT.

Brightstar N.V. - Know Your Client (KYC), Anti-Money Laundering (AML), Counter Terrorist Financing (CTF) and Combating Financing of Proliferation (CFP) policy & procedures

- **Senior Management:** All executive team members and department heads responsible for oversight and strategic implementation of AML/CTF/CFP procedures.
- **The Money Laundering Reporting Officer (MLRO):** The designated individual responsible for implementing and overseeing compliance with AML/CTF/CFP frameworks.
- **Third-Party Suppliers and Service Providers:** Including but not limited to payment processors, software providers, and identity verification vendors involved in customer onboarding, transaction processing, or data storage.
- **Subcontractors and Consultants:** Any individual or business entity engaged under a subcontract or consultancy agreement with Brightstar N.V. who may access customer information, financial data, or contribute to regulated processes.
- **Customers (Players):** End-users of Brightstar N.V.'s gaming services whose identification, financial transactions, and behaviors are subject to verification and monitoring under AML/CTF/CFP standards.

All parties are expected to adhere strictly to the contents of this policy and ensure full cooperation with Brightstar N.V.'s compliance and reporting mechanisms.

1.3 DEFINITIONS

For the purposes of this policy, the following terms shall have the meanings ascribed below:

- **Money Laundering:** The process of concealing the origins of illegally obtained money, typically by means of transfers involving foreign banks or legitimate businesses. It involves three key stages: Placement, Layering, and Integration.
- **Terrorist Financing:** The provision or collection of funds, by any means, intended to be used to carry out terrorist acts. It can involve both legitimate and illicit sources and follows the phases of Collection, Transmission, and Use.
- **Proliferation Financing:** The act of providing funds or financial services used, wholly or in part, for the manufacture, acquisition, or use of nuclear, chemical, or biological weapons, in contravention of national or international laws.
- **Politically Exposed Person (PEP):** An individual who is or has been entrusted with prominent public functions, including heads of state, senior politicians, senior government or judicial officials, military officers, and executives of state-owned enterprises. Includes their immediate family members and close associates.
- **Customer Due Diligence (CDD):** The process of identifying and verifying the identity of customers, assessing risk, and monitoring for suspicious behavior, particularly in relation to financial crime.
- **Enhanced Due Diligence (EDD):** Additional verification measures applied to higher-risk customers, such as PEPs or those from high-risk jurisdictions, to further assess identity, source of funds, and source of wealth.
- **Sanctions Screening:** The process of comparing customer information against national and international sanctions lists, including those published by the UN, EU, and OFAC.
- **Suspicious Transaction Report (STR):** An internal report submitted to the MLRO when there is knowledge, suspicion, or reasonable grounds to suspect money laundering or terrorist financing.

Brightstar N.V. - Know Your Client (KYC), Anti-Money Laundering (AML), Counter Terrorist Financing (CTF) and Combating Financing of Proliferation (CFP) policy & procedures

- **Suspicious Activity Report (SAR):** A formal report submitted to the Financial Intelligence Unit (FIU) when a suspicious transaction is identified and confirmed by the MLRO.
- **Threshold Approach:** A framework where specific transaction amounts trigger verification steps, such as KYC and EDD requirements.
- **Customer Risk Assessment:** The categorization of customers as low, medium, or high risk based on factors such as geography, transaction behavior, and verification status.

1.4 POLICY APPROVAL AND OVERSIGHT

This policy has been reviewed and approved by the designated senior official(s) responsible for Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Combating the Financing of Proliferation (CFP) compliance within Brightstar N.V.

The primary approving authority for this policy is:

- **Nwankwo Chibuikwe Chinonso Justice**, Money Laundering Reporting Officer (MLRO)
Responsible for the development, implementation, and oversight of the Company's AML/CTF/CFP framework.

Policy updates, including compliance with new laws, guidelines, and risk mitigation strategies, will be approved by the MLRO in collaboration with senior management.

The next scheduled review of this policy is April 14, 2026. Major revisions or first-time implementations will undergo review within one year. Thereafter, the policy shall be reviewed at a minimum every three years, or earlier as necessary.

All future revisions of this policy will be reviewed and formally signed off by the MLRO and, where appropriate, escalated to the Board of Directors for final approval.

1.5 RESPONSIBLE OFFICE

The **Compliance Department** is designated as the Responsible Office for the implementation, dissemination, ongoing review, and periodic updating of this AML/CTF/CFP Policy. This includes:

- Ensuring the policy is effectively communicated and accessible to all relevant employees, contractors, and stakeholders;
- Reviewing the policy at least annually and following any legislative or regulatory changes;
- Coordinating with the Money Laundering Reporting Officer (MLRO) to ensure updates reflect emerging risks and updated best practices;
- Ensuring all policy changes are approved by the appropriate senior official(s) and documented in the version control log.

The Compliance Department, under the direction of the MLRO, ensures that all staff Brightstar N.V. - Know Your Client (KYC), Anti-Money Laundering (AML), Counter Terrorist Financing (CTF) and Combating Financing of Proliferation (CFP) policy & procedures

receive appropriate training and that the policy remains fit for purpose in preventing money laundering, terrorist financing, and the financing of proliferation.

1.6 COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

Brightstar N.V. is committed to full compliance with applicable Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Combating Financing of Proliferation (CFP) regulations. Failure to adhere to this policy exposes the Company, its employees, and its partners to serious legal, regulatory, and reputational risks.

1.6.1 Employee Non-Compliance

Employees who fail to comply with this policy — whether intentionally or through negligence — may face:

- Formal warnings
- Mandatory retraining or reassignment
- Suspension or dismissal from their role
- Internal investigation and reporting to external authorities

Deliberate non-compliance or willful blindness may also result in **criminal liability**, depending on the nature and severity of the breach.

1.6.2 Third Parties and Suppliers

All third-party service providers, subcontractors, and consultants are expected to uphold the principles outlined in this policy. Breaches by third parties may result in:

- Immediate contract termination
- Withholding of payments or services
- Reporting to competent authorities or regulators

1.6.3 Customer Non-Compliance

Customers who violate AML or KYC obligations (e.g., submitting fraudulent documents, attempting to circumvent limits, or engaging in suspicious transactions) may face:

- Account suspension or permanent closure
- Freezing of funds and/or reporting to the Financial Intelligence Unit (FIU)
- Involvement of law enforcement agencies

1.6.4 Business Risks

Failure to comply with AML/CTF/CFP obligations can result in:

- Regulatory fines and sanctions
- License revocation or suspension
- Reputational damage impacting player trust, partnerships, and market presence
- Legal proceedings or criminal prosecution

Brightstar N.V. - Know Your Client (KYC), Anti-Money Laundering (AML), Counter Terrorist Financing (CTF) and Combating Financing of Proliferation (CFP) policy & procedures

Brightstar N.V. enforces a **zero-tolerance policy** regarding any form of non-compliance and reserves the right to take all necessary steps to protect its operations, licenses, and reputation.

1.7 RELATED INFORMATION

This policy is supported by a broader compliance framework and references the following related documents, legal instruments, and resources. All listed items should be reviewed and understood in conjunction with this AML/CTF/CFP policy.

Internal Policies and Documents

- **Customer Acceptance Policy**
Details customer onboarding procedures, risk categorization, and account monitoring standards.
- **Business Risk Assessment (BRA)**
Evaluates the Company's overall exposure to financial crime risks and outlines mitigating controls.
- **Terms and Conditions of Brightstar N.V.**
Contractual agreement governing the relationship between the customer and the Company.

Sanctions Lists

- **United Nations Consolidated Sanctions List:**
<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>
- **European Union Sanctions Map:**
<https://www.sanctionsmap.eu/#/main>
- **OFAC Sanctions List Search (U.S. Department of the Treasury):**
<https://sanctionssearch.ofac.treas.gov>

Regulatory Guidelines

- **Curacao Gaming Control Board (GCB) AML/CTF Guidelines**
<https://gamingcontrolcuracao.org>

Other Tools & Templates (Internal Use)

- Suspicious Transaction Report (STR) Template
- AML Compliance Training Log
- Delegation of AML Responsibilities Register

1.8 CONTACT INFORMATION

For any questions, clarifications, or concerns regarding this AML/CTF/CFP policy, please contact:

Compliance Department

Brightstar N.V.

✉ Email: compliance@brightstarnv.com

The Compliance Department is responsible for providing guidance on the implementation of this policy, answering questions related to regulatory obligations, and supporting internal training and reporting procedures.

2.0 OBJECTIVES

The objective of this policy is to establish and implement a comprehensive framework for Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Combating the Financing of Proliferation (CFP) within Brightstar N.V. It defines the procedures, roles, and responsibilities required to ensure compliance with Curaçao's legal and regulatory obligations, including the guidance issued by the Curaçao Gaming Control Board (GCB) and relevant international standards.

This policy outlines how Brightstar N.V. identifies, assesses, and mitigates financial crime risks through an integrated approach that includes customer due diligence (CDD), enhanced due diligence (EDD), transaction monitoring, sanctions screening, staff training, and internal reporting procedures. It also addresses the escalation of suspicious activity, the governance framework for policy oversight, and the implementation of effective internal controls based on ongoing risk assessments.

Brightstar N.V. is committed to preventing its services from being used to facilitate money laundering, terrorist financing, or the proliferation of weapons of mass destruction. This commitment supports the Company's broader objective of maintaining the integrity and transparency of its operations, protecting customers and stakeholders, and ensuring that its platform is not associated with criminal or fraudulent activity.

3.0 THE MEANING OF MONEY LAUNDERING

Money laundering is the process of illegally disguising the origin of money obtained from illicit activities, such as drug trafficking, corruption, embezzlement, or terrorism, so that it appears to have come from a legitimate source.

Money laundering occurs every time any transaction takes place, or any relationship is formed that involves any form of property that has come from any crime.

The key objectives for money launderers are to:

- Disguise the source of criminal property.
- Conceal / distance ownership of criminal property but still keep control of it;
- Avoid detection for the underlying crimes; and
- Benefit from the proceeds of crime securely.

3.1 HOW IS MONEY LAUNDERED?

AML law and regulation identifies “customer not present” transactions (i.e., there is no face-to-face contact), which applies to remote gambling, as high risk and therefore should be managed as high risk. Money laundering may take a variety of forms and use a number of methods using multiple financial services and products. Traditionally the money laundering process comprises three main stages, following a predicate crime, whereby proceeds of crime are obtained:

1. Placement – where cash from criminal activity is placed into the financial system. For Brightstar N.V. this would be at the point when a customer deposits.
2. Layering – Which usually involves a complex system of transactions designed to hide the source and ownership and confuse authorities. For Brightstar N.V. this could for example relate to customers betting equally on red and black on roulette or creating multiple accounts;
3. Integration – where laundered funds are reintroduced into a legitimate economy, appearing to have come from a legitimate source. For Brightstar N.V. this would be when customers withdraw funds from their account.

It is important to add, here, that customers may use the remote gambling industry to launder funds, not in the conventional way of laundering funds (placement, layering and integrating), but by simply spending funds with remote gambling operators that were illegally obtained (e.g., theft, fraud, etc.).

4.0 TERRORIST FINANCING

Terrorist financing is a general term to describe activity that provides or facilitates the provision of money or property to be used for terrorist purposes.

Traditionally, AML efforts have concentrated on the criminalization of the laundering of the proceeds of different forms of underlying criminal conduct. Terrorist financing is a serious threat to financial businesses or businesses where a high volume of monetary transactions take place. This threat must be taken as seriously as money laundering.

The mainstream methods to raise funds used by terrorist organizations include:

Brightstar N.V. - Know Your Client (KYC), Anti-Money Laundering (AML), Counter Terrorist Financing (CTF) and Combating Financing of Proliferation (CFP) policy & procedures

- Private donations by terrorist supporters / sympathizers
- Abuse and misuse of non-profit organizations and charities
- Criminal activity
- Legitimate commercial activity
- Infiltration into companies/ organizations

Terrorist financing often involves a complex series of transactions; like money laundering, this generally follows three separate phases:

1. Collection – funds are often acquired through seeking donations, carrying out criminal acts, or diverting funds from genuine charities.
2. Transmission – where funds are pooled and transferred to a terrorist or terrorist group.
3. Use – where the funds are used to finance terrorist acts, training, materials, accommodation, propaganda, etc.

This 3-phase approach is vastly similar to that of more “traditional” money laundering activity. It is therefore important to focus on the same areas whereby an individual has knowledge, suspicion, or reasonable grounds to suspect illicit activity of some kind.

5.0 FINANCING OF PROLIFERATION

Proliferation financing is being defined as “the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.”

The proliferation of weapons of mass destruction can take many forms, but ultimately involves the transfer or export of technology, goods, software, services, or expertise that can be used in programs involving nuclear, biological, or chemical weapons and their delivery systems (such as long-range missiles).

6.0 RESPONSIBILITIES

6.1 TRANSACTIONS MONITORING

The Compliance department is responsible for monitoring all transactions to and from Brightstar N.V. and for verifying the identity of all online registered players. Brightstar N.V.'s Senior management, as well as all employees are fully committed to adopting a risk-based approach to anti- money laundering ("AML") with an effort focused where it is most needed, to be able to process payment transactions between Brightstar N.V. and the customers of our Casino in a safe way, free of money laundering issues.

The development of internal systems and procedures applied by Brightstar N.V. are appropriate for remote gaming businesses.

The Company appreciates that its money laundering and terrorist financing risk assessment is not a one-off exercise, and these are assessed regularly so that adopted approach is effective at any time.

Further information on the monitoring of transactions can be found in Brightstar's *Customer Acceptance Policy*.

6.2 TIPPING OFF

One key responsibility across all employees is that tipping-off must not take place at any stage.

Any account under investigation must be treated with a special care and tipping off must be avoided: we cannot let any individual under potential money laundering investigations, unusual transactions, or regulatory reporting know about the suspicion or investigation.

6.3 SENIOR MANAGEMENT RESPONSIBILITY

Senior management is fully engaged in the processes around Brightstar N.V. assessment of risks for money laundering and terrorist financing and are involved at every level of the decision making to develop the appropriate policies and processes to comply with relevant legislation.

6.4 MONEY LAUNDERING REPORTING OFFICER (MLRO)

The MLRO is responsible for the oversight of all aspects of the AML activities within the company and has the authority to act independently in carrying out his/her

Brightstar N.V. - Know Your Client (KYC), Anti-Money Laundering (AML), Counter Terrorist Financing (CTF) and Combating Financing of Proliferation (CFP) policy & procedures

responsibilities, having access to sufficient resources to carry out his/her duties.

His/her duties and responsibilities include:

- Identifying money laundering and terrorist financing risks relevant to the Company;
- Designing and implementing policies and procedures relating to AML and countering terrorist financing (“CTF”), monitoring the effectiveness of these and reviewing and updating these policies and procedures;
- Reporting to Senior Management on AML and CTF activity and the effectiveness of the Company’s controls;
- Keeping AML/CTF/CFP records;
- Receiving internal disclosures and deciding whether these should be reported;
- Training employees to ensure that they are aware of the Company’s AML policies and procedures and how to report suspicious transactions;
- Being the internal point of contact for the suspicious transaction reports (“STRs”);
- Reviewing and investigating STRs and considering whether a suspicious activity report (“SAR”) should be submitted to the authorities.

Any internal report should be considered by the nominated officer, in light of all other relevant information, to determine whether or not the information contained in the report leads them to form knowledge or suspicion, or reasonable grounds for knowledge or suspicion, of money laundering or terrorist financing.

Where any AML tasks are delegated within the business, the MLRO will remain responsible for all AML issues. Any delegated tasks will be recorded and will be counter-signed by the delegate to confirm acceptance of responsibility. Employees who need to be aware of the delegation will be notified immediately.

6.5 EMPLOYEE’S RESPONSIBILITIES

Employees are trained to follow Brightstar N.V. policies and procedures for customer due diligence. Employees must report to the MLRO any knowledge or suspicion of money laundering whether by customers, guests, or other employees by drafting an internal STR.

7.0 CUSTOMER DUE DILIGENCE

Identifying a customer means obtaining information about his identity (name, address, date of birth, employment and financial history, physical appearance, and family circumstances). Verifying identity means obtaining evidence that supports this information. The Commission’s guidance sets out that it generally considers it a good

Brightstar N.V. - Know Your Client (KYC), Anti-Money Laundering (AML), Counter Terrorist Financing (CTF) and Combating Financing of Proliferation (CFP) policy & procedures

practice to require either:

- One government document which verifies either name and address or name and date of birth; or
- A government document which verifies the customer's full name and another supporting document which verifies their name and either their address or date of birth.

CDD is carried out to identify and verify the identity of all customers. Brightstar N.V. is aware that CDD is ongoing and may need updating where there are changes in a customer's circumstances and personal details.

The CDD process is complete when a customer provides Brightstar N.V. with his/her name, residential address, photo and date of birth Identification Documents, details of source of income and, in some circumstances when requested by the Payment Department, a copy of the payment method used or to be used by the customer.

When CDD checks on an existing customer have been completed within one of Brightstar N.V. products, CDD will not be conducted again in relation to another product unless a different payment method is used by the customer, or the documents or information are not valid anymore.

Records of CDD are kept for ten years from the end of the business relationship or the customer's last visit to our website.

7.1 CUSTOMER REGISTRATION

In order to open an account with Brightstar N.V. at the web portal, the customer must first complete the registration process and accept the Terms and Conditions.

The registration details to be filled in by all new customers include password, first and last name, address, country of residence, date of birth, and email address. During registration, customer identification takes place by way of the age verification process. As per the Company's T&Cs, the details provided need to be correct and accurate. Players found to provide false information may face account suspension or termination.

Customers will not be able to register with fictitious names or anonymous accounts. An account will not be opened unless the requested identity details are completed in full. Duplicate accounts are strictly prohibited, and checks will be conducted at the time of registration to prevent multiple accounts.

Obvious fictitious names will be flagged, especially when funds are deposited, and such accounts will be terminated. A participant whose account is terminated will be notified via email unless the termination relates to a matter reported to the FIU, in which case further action will be determined by the MLRO.

When a new account is created, a verification link is sent to the email account specified during the registration process. When the user clicks on the link, the account is then successfully created. Only at this point can the customer deposit money and start placing bets.

Customers must be at least 18 years old and are permitted to register only one player account in their name. No underage users are allowed to play on the website. The system is designed not to accept underage players and to deny registration if the year of birth is below the minimum legal age for gambling.

Brightstar N.V. is committed to preventing underage individuals from using its gambling facilities and will take all necessary steps to ensure they do not register with its remote gaming website. Users who do not have a registered player account will not be allowed to play casino games or place bets.

7.2 SANCTIONS SCREENING

With the information provided at customer registration, Brightstar N.V. will conduct the initial mandatory screening of the customer against international sanctions lists. To comply with current legislation and to avoid aiding criminals, particularly in money laundering and terrorist financing intentions, we will constantly check our complete customer database against the most important sanctions regimes. This includes the United Nations (UN), European Union (EU), and Office of Foreign Assets Control (OFAC) sanctions lists. In case there is any hit on a sanction list, we will immediately freeze the customer's account, end the relationship, and file the necessary reports to the Regulator and/or the FIU.

Sanctions are restrictions used by international communities as part of an attempt to stop financial crime and terrorism. They are designed to change the behavior of a targeted country, regime, or individuals where diplomatic efforts have failed. Sanctions can take the form of economic, trade, financial services, or international movement (travel bans) prohibitions. Targeted financial sanctions require countries to freeze funds and assets and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of any designated persons or entities.

UN Sanctions

The United Nations Security Council publishes the names of individuals and organizations subject to UN financial sanctions in relation to involvement with ISIL (Da'esh), Al-Qaeda, and the Taliban. All UN member states are required under international law to freeze the funds and economic resources of any legal person(s) named in this list and to report any suspected name matches to the relevant authorities. The UN also has other sanction lists related to jurisdictions, entities, and individuals involved in broader terrorist activities under UNSR 1373.

The UN consolidated sanctions list is available at the following link:

<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

EU Sanctions

The European Union applies sanctions or restrictive measures in pursuit of the specific Common Foreign and Security Policy (CFSP) objectives set out in the Treaty of the European Union. These measures may incorporate UN Security Council sanctions or EU autonomous sanctions, which cannot be imposed against individuals or entities without a foreign policy dimension.

The EU sanctions regimes can be accessed here:

<https://www.sanctionsmap.eu/#/main>

The above-mentioned website also includes information about UN sanctions regimes.

OFAC Sanctions

The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals. These sanctions target foreign countries and regimes, terrorists, international narcotics traffickers, and those involved in activities related to the proliferation of weapons of mass destruction. While US sanctions do not directly apply to non-US companies outside the US, the use of the US dollar in transactions may engage OFAC regulations. US prosecutors take the view that if a financial transaction has cleared in the US (as do all US dollar payments, in New York), the US has jurisdiction over the offence.

OFAC publishes a list of 'Specially Designated Nationals' (SDNs) whose assets are blocked, and US persons are generally prohibited from doing business with them.

The OFAC Sanctions List Search is available here:

<https://sanctionsssearch.ofac.trcas.gov/>

The system also checks the provided details and screens against PEP matches. Registration will also be denied if a PEP match is confirmed.

Automatic checks are completed to establish if the registered details match with any of the details added to the Company's internal blacklists. If a match is detected, then registration is not allowed.

Additional security checks: the system automatically checks and blocks registration of accounts which use VPNs, anonymizers or try to register from a country which is not allowed by the Regulator. The system also runs duplicate and related account automatic checks based on Device and IP.

7.3 POLITICALLY EXPOSED PERSONS (PEPs)

A Politically Exposed Person (PEP) is generally considered to present a higher risk to a business with whom they are transacting due to being considered more vulnerable to bribery and corruption. Therefore, full enhanced due diligence (EDD) must be conducted upon any identified PEPs. The Company does not distinguish between foreign and domestic PEPs; all are considered high risk. A PEP that no longer holds their prominent public role will also be deemed high risk.

Screening is undertaken by the Company with the help of Refinitiv World Check to identify PEPs and sanctioned individuals upon customer registration and deposit. This screening process will also detect any adverse media relating to the customer.

Definition of a PEP

A PEP is defined as a natural person who is or has been entrusted with prominent public functions, including:

- A head of state, head of government, minister, or deputy/assistant minister;
- A senior government official;
- Member of Parliament (MP);
- A senior politician;
- An important political party official;
- A senior judicial official;
- A member of a court of auditors or the board of a central bank;
- An ambassador, chargé d'affaires, or other high-ranking officer in a diplomatic service;
- A high-ranking officer in an armed force;
- A senior member of an administrative, management, or supervisory body of a state-owned enterprise;
- A senior official of an international entity or organization.

Family Members and Close Associates of PEPs

A PEP also includes family members and close associates of the above, including:

- A spouse;
- A partner considered by national law as equivalent to a spouse;
- Other known close personal relationships such as a partner, boyfriend, or girlfriend;
- A child;
- A spouse or partner of a child;
- A brother or sister (including a half-brother or half-sister);
- A spouse or partner of a brother or sister;
- A parent;
- A parent-in-law;
- A grandparent;
- A grandchild;
- A joint beneficial owner of a legal person or legal arrangement, or any other close business relationship, with a PEP;
- The sole beneficial owner of a legal person or legal arrangement known to have been set up for the benefit of a PEP;
- A beneficiary of a legal arrangement of which a PEP is a beneficial owner or beneficiary;
- A person in a position to conduct substantial financial transactions on behalf of a PEP.

Brightstar N.V. ensures that all PEP-related transactions undergo thorough scrutiny to mitigate risks associated with bribery, corruption, and financial crime.

7.4 THRESHOLD APPROACH

Brightstar N.V. adheres to regulatory requirements by implementing customer due diligence (CDD) measures at specific transaction thresholds. The Company ensures compliance through a structured verification process based on cumulative transaction amounts and customer behavior.

KYC verification is triggered when a player reaches any of the following thresholds:

- Upon the player's first withdrawal request: A government-issued ID and a bank statement are mandatory at this threshold.
- Upon reaching EUR 2,000 in cumulative transactions: A government-issued ID, a utility bill or bank statement, and copies of the cards/wallets used for deposit must be provided. The threshold is calculated daily, taking into account all deposits, withdrawals, and peer-to-peer transfers.
- If there are suspicions of Fraud/AML/RG/Compliance violations: (e.g., suspected third-party credit card usage, identity theft, bonus abuse, or other suspicious

activities), the customer must provide additional documentation, including a government-issued ID, a selfie with an ID document, a utility bill or bank statement, and copies of the cards/wallets used for deposit.

- Upon detecting an *unusual transaction*.

Once the EUR 2,000 threshold is met, Brightstar N.V. ensures that:

- A customer risk assessment is conducted;
- Full CDD measures are applied in accordance with the customer's risk level;
- Enhanced due diligence (EDD) is carried out where necessary.

If a customer reaches the EUR 2,000 threshold due to a deposit, they will not be able to deposit or withdraw additional funds until verification is successfully completed. However, they may continue to play using their existing balance.

If the EUR 2,000 threshold is reached due to a withdrawal request, the customer's account will be restricted, preventing further transactions until verification is completed.

Unusual Transactions

Each transaction or series of transactions that amounts to EUR 2,500 or more is considered an unusual transaction and will trigger further verification. The customer must provide a government-issued ID, a utility bill or bank statement, and copies of the cards/wallets used for deposit.

Brightstar N.V. considers the following transactions or intended transactions as unusual transactions:

- Transactions linked to money laundering or terrorism financing that are reported to the Police or the Department of Justice.
- Transactions involving individuals or entities listed under the Sanctions National Ordinance (N.G. 2014 no. 55).
- Transactions in the amount of EUR 2,500 or more, whether conducted via electronic transfer, or other non-physical means. This includes but is not limited to:
 - A withdrawal of EUR 2,500 or more, which refers to a transfer from our casino's bank account to a local or international bank account at the request of the client.
 - Accepting a deposit in the amount of EUR 2,500 or more at the request of the client.

A transaction may consist of a single event or a series, combination, or pattern of transactions that, when aggregated, meet or exceed EUR 2,500 per gaming day. These transactions are subject to enhanced scrutiny and verification procedures to ensure compliance with AML/CFT regulations.

Brightstar N.V. does not accept deposits exceeding EUR 2,000 per transaction and does not process withdrawals exceeding EUR 2,000 within a single day. Any attempt to circumvent these limits by making multiple transactions will be flagged for review and may be subject to further verification and compliance measures.

7.5 PERSONAL DETAILS ADJUSTMENT

To ensure compliance and protect the integrity of the player database, personal information updates are restricted as follows:

Name, Gender, DOB, Address and Phone number Adjustments

- Changes to these details require submission of a written request and valid government-issued documents by the account holder
- The player must go through the verification process again to confirm that the new details are legitimate.
- The Fraud and KYC team will process the request and update the player profile upon successful validation.

7.6 DOCUMENTARY EVIDENCE

Brightstar N.V. relies upon documents issued by government departments during CDD.

To fulfil the necessary customer identification and verification process, Brightstar N.V. requires its customers to upload on our website (under My account -> Verification) a copy of valid identification documents. This request is communicated to the customer via the email address registered. If necessary, the customer may be contacted by phone to further facilitate and continue the verification process. If documents are in a foreign language, Brightstar N.V. takes appropriate steps to be reasonably satisfied that the documents provide evidence of the customer's identity, for example, by obtaining a translation of the relevant sections. Such a step would be to request that the customer provides the documents with a certified true translation.

Only documents issued by government departments and agencies that contain a photograph are considered reliable to verify the customer's identity. Government issued documents without a photograph may be used to confirm the current address of the customer (if stated on the document).

The following sources may be accepted for verification of customers:

- Valid passport or ID card
- Birth certificate;
- Valid photo card driving license;
- Residence permit issued by a governmental institution;
- Utility bill or statement (but not website print outs), or a certificate from a utility's supplier confirming an arrangement to pay services on pre-payment terms;
- Bank, building society or credit union statement or passbook containing current address but not statements printed off the internet) – bank or credit cards alone will not be sufficient as these do not provide either residential address or date of birth.

7.7 ENHANCED DUE DILIGENCE

Under the Regulations, there are three circumstances in which EDD on customers should be carried out, which goes beyond identifying them and verifying their identity. These are:

- When the customer is a PEP or RCA (Relatives and Close Associates);
- In any other situation where the customer presents a higher risk of money laundering or terrorist financing (e.g., a high spending customer).
- In any other situation where the customer presents any potential fraud risk.

Customers from High-Risk Jurisdictions

A customer located in a jurisdiction that is not compliant with the Financial Action Task Force (FATF) standards (i.e., listed on FATF's Black or Grey List) may generally be considered to represent a heightened risk of money laundering or terrorist financing activity. Therefore, customers located in jurisdictions named within the Blacklist will be automatically subjected to enhanced due diligence and subject to a higher degree of ongoing monitoring.

This includes:

- More stringent verification processes;
- Additional documentation requirements to verify the customer's identity and source of funds;
- More frequent transaction monitoring and scrutiny of financial behavior;
- Potential limitations on account activity until verification requirements are satisfied.

The FATF regularly updates its lists of high-risk jurisdictions, and Brightstar N.V. will ensure that its procedures reflect these updates in real time to mitigate exposure to financial crime risks.

Brightstar N.V. - Know Your Client (KYC), Anti-Money Laundering (AML), Counter Terrorist Financing (CTF) and Combating Financing of Proliferation (CFP) policy & procedures

EDD Procedures

In relation to PEPs and other customers that present a higher risk of money laundering or terrorist financing, Brightstar N.V. will apply different EDD measures to establish reliable risk / wealth profile for the customer. Sometimes this will include obtaining evidence of the customer's source of funds and source of wealth.

This evidence may include but are not limited to:

- Identification documents provided by the customer (e.g., passport, driving license, utility bill)
- Self-certified ID
- Business cards provided by the customer;
- Information provided by the customer in conversation/correspondences;
- Verification of identity using an online provider;
- Third party acuity and wealth reports;
- Credit reports;
- Information available in the media and on the internet;
- Search of PEP databases;
- Company registration searches for companies the customer appears to be a shareholder or officer of.
- SOF / SOW documentation – payslip, Company documents, Bank Statements showing certain transactions and others.

Brightstar N.V. will use a variety of sources, including external sources and information taken directly from the customer, for EDD purposes.

7.8 REQUIREMENTS PROCEDURES

In the light of the requirements imposed by law and regulations, Brightstar N.V. adopt the following procedure when CDD and EDD are triggered under the threshold approach:

- At the point that ID verification is triggered, Brightstar N.V. puts all funds owed to the customer into account (or equivalent) from which no withdrawals can be made;
- Further deposits can be made to that account, provided they are also 'locked' until CDD is completed.
- Bets can be placed from the account, but any winnings will remain 'locked' until CDD is completed.
- Once CDD is completed, the account can be 'unlocked' and business can resume as normal. If CDD cannot be completed, Brightstar N.V. will restrict the customer's account.
- There will be appropriate risk mitigation.

Brightstar N.V. - Know Your Client (KYC), Anti-Money Laundering (AML), Counter Terrorist Financing (CTF) and Combating Financing of Proliferation (CFP) policy & procedures

Upon triggering certain deposit or loss thresholds, a risk assessment is undertaken on the customer. Based on comprehensive account review, each account is categorized as low, medium or high risk. EDD is applied immediately to all high-risk customers, and it includes asking for SOF/SOW documents when deemed necessary. The accounts falling under the low or medium risk category are monitored on a regular and ad hoc basis and the risk level can be changed when needed.

The risk level is determined based on different factors, including but not limited to:

- PEP status
- Adverse media
- Appearance in sanction lists
- Location
- Verification status
- Account lifetime duration
- Online information found, including occupational information and estimated income
- Financial history – deposit, WD and loss amounts, patterns, average deposit, velocity, etc.
- Gameplay

7.9 FAILURE TO COMPLETE CHECKS

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

While the verification process is ongoing, the customer may continue using their account; however:

- 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 threshold is met due to a withdrawal request, the account will be restricted, preventing further transactions until verification is successfully completed.

If the required documentation is not received within 30 days of reaching the threshold, Brightstar N.V. will:

- Restrict or terminate the business relationship with the customer;
- Report the transaction to the FIU if there is suspicion of money laundering or terrorist financing;
- If no suspicion of financial crime exists, return the funds to the original deposit source.

Where suspicion of money laundering or terrorist financing arises, internal procedures

Brightstar N.V. - Know Your Client (KYC), Anti-Money Laundering (AML), Counter Terrorist Financing (CTF) and Combating Financing of Proliferation (CFP) policy & procedures

will determine whether funds should be blocked, taking into account the risk of "tipping off" the customer.

7.10 KYC MATRIX

Brightstar N.V. applies a risk-based approach to Customer Due Diligence (CDD), ensuring that the level of verification is proportional to the level of risk presented by a customer. The following matrix outlines the required due diligence checks based on the customer's risk level:

Due Diligence Check	Low Risk	Medium Risk	High Risk
PEP, Sanction, Adverse media screening	✓	✓	✓
Identity Verification Screening	✓	✓	✓
Request ID and Address Documents	✓	✓	✓
Open-Source Checks	✓	✓	✓
Source of Funds		✓	✓
Source of Wealth			✓
Additional Identity Documents			✓

The risk level is determined based on various factors, including transaction history, customer behavior, geographical risk, and regulatory requirements. Our Company conducts ongoing monitoring to ensure compliance and to detect any changes in customer risk profiles.

More information on the risk assessment can be found in Brightstar N.V.'s *Business Risk Assessment*.

7.11 ONGOING MONITORING OF IDENTITY

Brightstar N.V. conducts **ongoing monitoring** of customer identity and personal information to ensure compliance with regulatory obligations and to mitigate risks associated with financial crime.

Review of Customer Identity Information

Any changes made to a customer's identity or personal details will be reported to the Compliance Department for review. The evidence of identity previously provided by the customer will be reassessed, and steps will be taken to update the information in light of the reported changes. In such cases, verification procedures will be followed, and the customer will be required to provide reasoning for the modification of their details.

Risk-Based Approach to Ongoing Monitoring

- If a customer's risk level increases (e.g., from low to medium risk), the Compliance Department will assess whether additional due diligence documents are required.
- Previously supplied documents must be reviewed to ensure they are still valid. If expired, updated documents must be requested.
- CDD/EDD records will be reviewed annually, regardless of any changes to the customer's circumstances, to ensure ongoing compliance.

Failure to Provide Updated Identity Verification

If a customer fails to provide satisfactory confirmation of identity or verification of updated identity documents, the following measures will be taken:

- The customer's account will be suspended;
- No further betting or gaming activity will be permitted;
- Consideration will be given to filing a Suspicious Transaction Report (STR) with the Financial Intelligence Unit (FIU) if deemed necessary.

7.12 OVERALL RISK ASSESSMENT

The *Business Risk Assessment* (BRA) is owned and managed by the Legal & Compliance function of the business, and primarily the Chief Legal & Compliance Officer. Whilst produced independently from other business lines, the BRA may form the basis for strategic actions which are owned and driven at Board level

The primary objective of this risk assessment is to enhance financial crime risk management by identifying general and specific money laundering and terrorist financing risks faced by Brightstar N.V. It evaluates how these risks are mitigated through internal controls and determines the residual risk exposure.

Following a comprehensive risk assessment, customers will be categorized as low, medium, or high risk, or they may be restricted from opening an account if they fail to meet regulatory requirements. The level of Customer Due Diligence (CDD) applied to each participant will correspond to their risk classification and will be subject to ongoing monitoring to detect any changes in behavior or risk exposure.

Full information on the overall risk assessment can be found in the *Business Risk Assessment* of Brightstar N.V.

8.0 ONGOING MONITORING

Monitoring customer activity is carried out using the risk-based approach, with higher risk customers, such as PEP's, being subjected to an appropriate frequency and depth of scrutiny, which is likely to be greater than is appropriate for lower risk customers.

Monitoring of customers is done by the relevant employees who monitor customer activity live and on an ongoing basis.

The ongoing monitoring of player activity is explained in detail in Brightstar N.V. *Customer Acceptance Policy*.

8.1 SUPPORTING RECORDS

We will, by the nature of our business, generate detailed records of all transactions with each customer and for the purpose of the record-keeping requirements Brightstar N.V. retains the drop/win figures for each named customer.

9.0 TRAINING

All relevant employees of Brightstar N.V. are given training on AML, CTF and CFP both at induction and by way of refresher training on an annual basis. Brightstar N.V. ensures that employees understand the Rules and Regulations and apply the Company's policies and procedures, including the requirements for CDD, record keeping and STRs/SARs.

The MLRO, nominated officers and employees responsible for completing CDD checks are regularly given training in how to recognize and deal with transaction and other activities which may be related to money laundering or terrorist financing.

10.0 KNOW YOUR EMPLOYEE

Complying with current international requirements related to AML and CTF means also understanding that besides looking out not to give access to criminals to our products and services, we also need to make sure our own employees are integer. AML / CTF Regulations are not only being followed because it's required by the law, but also because we are integer Company. We expect a high standard of integrity from our employees, so we perform background checks prior to hiring them. These checks will be performed on a risk-based approach commensurate to the employees' function, roles and responsibilities and authorization levels within the Company. This process is jointly owned by Compliance and HR.

11.0 RECORD KEEPING AND DATA SECURITY

Brightstar N.V. ensures that all customer-related records are maintained in a secure and accessible format, complying with regulatory obligations for anti-money laundering (AML), counter-terrorist financing (CTF), and responsible gaming monitoring. Secure backups of customer data are conducted daily.

Records Maintained:

- Customer Interactions:
 - Details of all customer interactions and relationships, including which

Brightstar N.V. - Know Your Client (KYC), Anti-Money Laundering (AML), Counter Terrorist Financing (CTF) and Combating Financing of Proliferation (CFP) policy & procedures

employee handled the interaction, the purpose, and the outcome.

- **MLRO Records:**
 - Decisions made when receiving an STR (Suspicious Transaction Report).
 - Training received from external organizations and provided to employees.
 - Details of AML tasks assigned to employees.
 - Reports submitted to the authorities.
 - Decisions made by authorities on SARs (Suspicious Activity Reports) and the subsequent actions taken.
- **Risk-Based Approach Documentation:**
 - Steps taken to manage and mitigate the risks of financial crime and disorder.
 - Customer identification and verification information, including copies of enhanced due diligence documentation.

Additional Record Keeping Obligations:

Brightstar N.V. also maintains the following records for compliance and operational purposes:

- **Customer Registration Details:**
 - Full registration information, identity verification details, standard and enhanced due diligence documentation.
- **Account Status:**
 - Suspended accounts and reasons for suspension, closed accounts, self-exclusion periods, self-imposed limits, and excluded players.
- **Financial Transactions:**
 - Deposits, bets made, withdrawals, and prize payments.
 - Bank reconciliations.
- **Compliance and Monitoring:**
 - Audit trails, complaints and responses, internal and external disclosures, register of money laundering and terrorist financing inquiries.
- **Customer Service Records:**
 - Electronic correspondence related to customer support interactions.

Retention Period:

- Customer records, including identification and financial transactions, will be retained for at least 5 years after the closure of the customer's account or the date of the last transaction.
- Records related to internal and external disclosures and money laundering inquiries will be maintained for 5 years following the finalization of the relationship with the related parties or for the period as advised by the Financial Intelligence Unit (FIU).

By maintaining these records, Brightstar N.V. ensures compliance with AML/CFT regulations and facilitates audits, investigations, and risk monitoring while safeguarding customer privacy and data security.

12.0 REPORTING

Where an employee of Brightstar N.V. has received information, as a result of which they know or suspect, or have reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing, that employee must make an internal report, an STR, to the MLRO.

Any STRs are considered by the MLRO, in light of all other relevant information, to determine whether or not the information contained in the report leads them to form knowledge or suspicion, or reasonable grounds for knowledge or suspicion, of money laundering or terrorist financing. Where appropriate, the MLRO will make an SAR to the relevant authority.

13.0 COLLUSION AND CHEATING

Brightstar N.V. has systems to detect cheating, collusion or illegal activity, including suspicious and large transaction alerts, risk management solutions to monitor customer transactions and online risk solutions. Where suspicious activity is identified, the customer's account will be reviewed, and this will be reported as an STR to the MLRO. The customer's account will be suspended and where cheating/collusion is identified, the account will be closed and the customer will be reported, where it is deemed necessary.

If an employee is implicated in any cheating, collusion or other illegal activity, they will be suspended pending a full investigation.

14.0 INDEPENDENT REVIEW

One of the pillars of a complete and well-functioning compliance program is the independent audit. The audit will be performed by an internal or external party as chosen by the Company. The most important requirement for this party is that it must

Brightstar N.V. - Know Your Client (KYC), Anti-Money Laundering (AML), Counter Terrorist Financing (CTF) and Combating Financing of Proliferation (CFP) policy & procedures

be independent from day-to-day compliance activities and not in charge of creating the AML CTF CFP Policies for the Company. This party must have AML / CTF / CFP Compliance knowledge. The scope of the audit is to assess whether Brightstar N.V. has met the requirements of a complete and robust compliance program and further whether this program is helping the Company to effectively combat money laundering and terrorist financing. The final report of this review process will be shared with the Board.

A handwritten signature in blue ink, appearing to be 'Menno Jordaan', is written over a horizontal line. The signature is stylized with a large 'X' shape.

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