

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	Steven Eisden (MLRO)
2.0	01.09.2024	Changes to policy in accordance with new Curacao regulations.	Steven Eisden (MLRO)

1.0 OBJECTIVES

The aim of this document is to define the Policy and Procedures in relation to Risk assessment and Management and involves a number of discrete steps in assessing how to manage and mitigate the money laundering and terrorist financing risks faced by Brightstar N.V. (“Brightstar N.V.” or the “Company”) by means of proper Know Your Client and Customer Due Diligence procedure. Brightstar N.V. is committed to prevent gambling from being a source of crime or disorder, being associated with crime or disorder, or being used to support crime.

2.0 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.

2.1 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.).

3.0 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:

- 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.

4.0 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).

5.0 RESPONSIBILITIES

5.1 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.

5.2 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.

5.3 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.

5.4 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 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.

5.5 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.

6.0 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 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 Inovaplay B.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.

6.1 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 e-mail 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.

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 the customer can 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 minimal legal age for gambling.

Brightstar N.V. is committed to preventing underage people 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.

6.2 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, European Union and 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.

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.

6.3 THRESHOLD APPROACH

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

- **Upon player's 1st withdrawal request:** Government-issued ID and a Bank statement are mandatory at this threshold.
- **Upon reaching EUR 2,000 cumulative lifetime deposits:** Government-issued ID, Utility bill or Bank statement and copies of the cards/wallets used for deposit are mandatory on this threshold.
- **Upon player requesting a "Big payment" (EUR 5,000 or more):** Government-issued ID, Utility bill or Bank statement and copies of the cards/wallets used for deposit are mandatory on this threshold.
- **In case of any suspicious of Fraud/AML/RG/Compliance issues (possible 3rd party CC usage; identity theft; bonus abuse, et.):** Government-issued ID, selfie with an ID document, Utility bill or Bank statement and copies of the cards/wallets used for deposit are mandatory on this threshold.

The identity of the player must be verified before processing the player's first withdrawal or upon reaching the EUR 2,000 deposit threshold.

If CDD cannot be completed, we reserve the right to block access to gambling facilities, deny further transactions to or from the customer or terminate business relationships.

The restrictions are determined on a risk-based approach.

6.4 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.

6.5 DOCUMENTARY EVIDENCE

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. 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.

6.6 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.

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.

6.7 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 as long as they too are 'locked' into it until CDD is completed\ bets can be made from the account, again providing any winnings are 'locked until CDD is completed;
- Bets can be made from the account, again providing any winnings are 'locked' until CDD is completed;
- Once CDD is completed, the account can be 'unlocked' and business can continue as normal\ if CDD cannot be completed, Brightstar N.V. will restrict customer's account.
- There will be appropriate risk mitigation.

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

6.8 FAILURE TO COMPLETE CHECKS

If a customer of Brightstar N.V. is unable to comply with or complete the required CDD or EDD within the timeframe allowed, Brightstar N.V. will not carry out a transaction with or for the customer through any of the available payment methods. Instead, the customer's account will be restricted, and Brightstar N.V. will consider making a report to the relevant authority (FIU) if there is any sign of a money laundering activity.

In case the customer decides to comply with the documents / information request at a later stage, the account can be reopened, and the business can continue as usual.

7.0 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.

7.1 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.

8.0 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

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

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.

9.0 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.

10.0 RECORD KEEPING

Brightstar N.V. will keep records of the following:

Customer interactions – Details of all customer interactions and relationships including which employee dealt with the interaction, what was asked, why an interaction was made and the outcome of the interaction.

MLRO – The decision made when receiving an STR, training received from external organizations and given to employees, details of AML tasks assigned to employees, reports sent to the authorities, decisions made by the authorities on SARs and the action that will be taken after the authorities have made their decision.

Risk-based approach - Details of steps taken to manage and mitigate risks of crime and disorder. Customer identification and verification information, including copies of any enhanced due diligence documentation.

These records will be kept for a period of at least ten years.

11.0 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.

12.0 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.

13.0 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 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.