

Prevention of Money Laundering and Terrorist Financing Manual of Betrust Entertainment B.V.

August 2024

Version	Date	Author/ Editor	Approver
1.0	31/08/2016	Compliance Officer	Board of Directors
2.0	31/08/2017	Compliance Officer	Board of Directors
3.0	31/08/2018	Compliance Officer	Board of Directors
4.0	31/08/2019	Compliance Officer	Board of Directors
5.0	31/08/2020	Compliance Officer	Board of Directors
6.0	31/08/2021	Compliance Officer	Board of Directors
7.0	31/08/2022	Compliance Officer	Board of Directors
8.0	31/08/2023	Compliance Officer	Board of Directors
9.0	31/08/2024	Compliance Officer	Board of Directors

Contents

Prevention of Money Laundering and Terrorist Financing Manual of..... 1

Betrust Entertainment B.V. 1

August 2024 1

1. Definitions 6

2. Statement..... 8

3. Purpose..... 9

4. Applicable Laws 9

5. Responsibilities 10

1.Board of Directors..... 10

2. Compliance Officer/Money Laundering Reporting Officer (CO/MLRO)..... 10

6. Risks..... 11

CUSTOMER RISK ASSESSMENT 13

A CRA has to be carried out either prior to the carrying out of an occasional transaction, or during the establishing of the business relationship. 13

7. Know Your Customer (Customer Due Diligence) 15

1. Basic CDD 16

7.2 ID 16

There are 3 different documents accepted as an Identity verification document: 16

- Picture/Scan of government-issued Identity Card with Picture, expiry date and signature:..... 16

o National ID..... 16

o Passport..... 16

o Driver’s License..... 16

- Once a document is received it should meet at least the following requirements: 16

o All 4 corners of the document should be clearly visible. 16

o All the Information displayed on the document needs to be clearly visible and readable (high resolution). 16

o The document should not be expired and must be a colored copy..... 16

On the bottom of the document is a machine-readable code that can be checked. 16

7.3 Proof of Address (PA)..... 16

The commonly accepted proof of address is: 16

o Picture/Scan of Electricity/Water/Gas bill. 16

o Picture/Scan of Internet Bill..... 16

o Picture/Scan of Landline phone bill (Mobile bill is not accepted)..... 16

o Picture/Scan of Letter from the bank or bank statement..... 17

Once a document received should also meet the below requirements: 17

○	Full document (All 4 corners visible)	17
○	Clear display of the issuing company, and date of issue of the document.....	17
○	Clear display of the name and address of the customer.	17
○	Date of issue within the last 3 months.	17
	7.4 Bank Cards	17
	For financial details verification when bank cards have been used requires:.....	17
❖	Front and back copies of each card used to be provided in accordance with the below requirements: .	17
○	Full document (All 4 corners visible).....	17
○	Of the 16 digits on the front the card; only the first 6 and the last 4 should be visible.	17
○	The CVV code should be hidden.....	17
○	All the other information should remain visible.....	17
5.	EDD.....	17
8.	Other Due Diligence.....	18
1.	B2B.....	19
2.	Third-Party Providers	19
3.	Ongoing Monitoring.....	19
4.	Retrospective	19
9.	Screening, Training and Awareness Program.....	19
	Persons working in the operation/ casino operated by Betrusted Entertainment B.V. are duly screened prior to entering the workforce for criminal records.	19
	Betrusted Entertainment B.V. provides training to all new employees and recurring refresher training for current employees to ensure they are aware of relevant subjects:	19
❖	Anti-Money Laundering and Counter Financing of Terrorism	19
❖	Fraud Prevention.....	19
❖	Information Security.....	19
❖	Responsible Gambling.....	19
❖	All training is managed, administered, and reported on by the MLRO.....	19
	The Payments and Customer Services team receives specialized training on monitoring customer registration, payment patterns, gambling activities, and personal information to detect indications of money laundering and respond appropriately to alerts or suspicions of money laundering or terrorist financing activities.	20
	All staff involved with customer accounts and activities on the platform are required to complete a training program to ensure they are fully aware of money laundering indicators and the available reporting structure. This program provides a comprehensive understanding of "normal" patterns and what constitutes suspicious or questionable activity deviating from this norm.	20
	Customer Service Representatives are not required, nor trained, to conduct investigative procedures, as their role is customer-centered. Requiring them to investigate customers would create a conflict.	20
	Yearly updates and refresher workshops are provided to existing staff to keep them informed of issues that have arisen and the ways these were resolved.	20
10.	Record Keeping and CIP.....	20
11.	Reporting Suspicious/Unusual Activities	20
1.	Suspicious Activity Report (SAR).....	20

12. Independent testing to the AML program 21

The AML compliance program must be monitored and evaluated at least annually by an independent internal audit department or an outside independent party. The testing encompasses the checking of compliance and adequacy of the relevant compliance procedures a.o.” 21

- evaluation of the casino’s AML, CTF, CFP manual;..... 21

- customer file review;..... 21

- compliance management;..... 21

- performance of transaction testing; 22

- assessment of training adequacy; 22

- assessment of compliance with relevant laws and regulations; 22

- evaluation of the system’s ability to identify unusual activity;..... 22

- assessment of the adequacy of the record retention system. 22

The result of the testing must be documented with any deficiencies reported to senior management with the request to take prompt corrective actions. 22

13. 22

12. High Risk Factors 22

1. PEP..... 22

2. PEP Log 22

3. Sanctions 22

4. Anonymous Accounts..... 23

5. Duplicate/Multiple/Shared Accounts..... 23

13. Cooperation with Regulators and Law Enforcement..... 23

12. Regular Review 23

This Policy will be reviewed on a regular basis to ensure that all the latest amendments to the money laundering regulations are kept up to date..... 23

This Policy will be reviewed and approved by the management board of Betrust Entertainment B.V. 23

13. Non-Compliance..... 23

1. Definitions

1. **ML:** Money Laundering:

1.1. All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source, can be considered money laundering (ML). It is the process of making dirty money look clean. Money Laundering consists of three phases:

1.1.1. Placement. During this stage, the money launderer introduces illegal proceeds into the financial system through financial institutions, casinos, shops and other cash-intensive businesses. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requests for payout and inserting funds into gaming machines and immediately claiming those funds as credits;

1.1.2. Layering. This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing money and hiding them from the authorities;

1.1.3. Integration. The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples are: the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments.

2. **UBO:** Ultimate beneficial ownership: the natural person(s) who ultimately own(s) or control(s) a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person.

3. **Company:** Betrust Entertainment B.V.

4. **Compliance Officer or Money Laundering Reporting Officer (MLRO):** A senior officer at management level and independent from the operations, responsible for the detection and deterrence of money laundering and terrorist financing.

5. **FATF:** The Financial Action Task Force. An independent intergovernmental body, established in 1989 and mandated by its Member Jurisdictions to develop and promote policies to protect the

global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

6. **FATF Recommendations:** A framework of recommendations on policies and measures, issued by the FATF, to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.
7. **Online gaming services:** Includes sports betting, esports-betting, fantasy sports, lottery and bingo, skill-based games and virtual sports.
8. **Board of Directors:** the board, committee, and/or body of an entity, which has the power to determine the strategy, objectives, and general direction of that entity and to oversee the management decision-making process, including the person who runs the business of that entity.
9. **Client:** Any natural person with a business relationship with the Company, also referred to in this Manual as ‘Player.’
10. **Business Relationship:** a relationship that is established upon conclusion of a long-term contract by an obliged entity in economic or professional activities for the purpose of provision of a service in another manner or that is not based on a long-term contract, but whereby a certain duration could be reasonably expected at the time of establishment of the contact and during which the obliged entity repeatedly makes separate transactions in the course of economic, professional or official activities while providing a service or official service.
11. **SOF:** Source of Funds: Refers to how the funds for a particular transaction were obtained by the player, like personal savings, pension release, property sales, share sales and dividends, gambling winnings, gifts, and compensation from legal rulings.
12. **SOW:** Source of Wealth: the origin of all the money a person has accumulated over their lifetime, like employment income, inheritances, investments, business ownership interests.
13. **FT:** Financing of Terrorism: the financing of terrorist acts, of terrorists and terrorist organizations. A terrorist act is an act to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

13.1. The most basic difference between financing of terrorism and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. Money laundering always involves the proceeds of illegal activity. There is a need for the terrorist group to disguise the link between it and its legitimate funding sources. In doing so, the terrorists use methods similar to those criminal organizations use to launder money like cash smuggling, structuring, wire transfers, purchase of monetary instruments, use of debit and credit cards. While ML is concerned with obscuring the source of funds, FT is mostly concerned with obscuring the end recipient of the funds.

14. **KYC:** Know Your Customer:

14.1. Verification of the identity of the customer

14.2. The requirement to gather information about the customer to be able to ascertain deviation from the “norm” that indicated suspicious activity

15. **PEP:**

15.1. Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country and direct family members or close associates of such people. Examples are Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

15.2. Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, and important political party officials.

15.3. People who are or have been entrusted with a prominent function by an international organization refer to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

2. **Statement**

Betrust Entertainment B.V., being a Curacao-licensed Gaming company, owning a European entity for transaction processing, is committed to maintaining the highest degree of integrity in all financial dealings with potential, current, and past customers, both in terms of normal commercial confidentiality, and the protection of all personal information received in the course of providing the company’s services concerned.

Our business is obliged to comply with European Union Anti-Money Laundering regulations in addition to any local laws that may apply to the jurisdiction in which the office is located.

We always conduct our services honestly and honorably and expect our customers and suppliers to do the same.

Apart from the more obvious offenses relating to drugs trafficking, terrorism, fraud, theft, or false accounting, consideration is also given to other potential offences which may well be encountered in business.

The policy applies to all Betrust Entertainment B.V. operations, group companies, and all player

accounts. The policy has been approved by the Board of Directors.

Failure to train staff on AML/CFT, failure to maintain customer records, or traceability funds are all breaches that may have severe consequences even when no crime or exploit has taken place.

3. Purpose

The purpose of this Manual is to ensure, that regardless of whether the undertakings of the Company might be in one country or different countries, adherence exist on a group-wide level to the Company's internal practice, measures, procedures and controls relevant to the prevention of Money Laundering and Terrorist Financing.

The Manual is developed and periodically updated by the Compliance Officer based on the general principles set up by the Company's Board of Directors about the prevention of Money Laundering and Terrorist Financing.

The Manual shall be communicated by the Compliance Officer to all the employees of the Company that manage, monitor, or control in any way the Clients' transactions and have the responsibility for the onboarding of Clients and for the application of the practices, measures, procedures and controls that have been determined herein.

This Policy will be reviewed and approved by the management board of the Company.

4. Applicable Laws

This present Manual was drafted in reference to best practice Principles and guidelines supplied from Several international Standards, directives, and acts, these include:

❖ Curaçao:

- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99)
- National Ordinance on Identification when Rendering Financial Services (NOIS) (N.G. 2017, no. 92)
- Sanctions National Ordinance (N.G. 2014 no. 55)
- Kingdom Sanction Act (N.G. 2016 no. 54)
- Sanction Ordinance Libya (N.G. 2015, no. 28)
- National decree for general measure of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance containing implementation of the UN's Security Council Resolution concerning Al-Qaeda, the Taliban of Afghanistan, ISIL, ANF and persons and organizations to be designated locally (N.G. 2015, no. 29)
- National Decree for general measures of the 10th of July 2015 for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the UN Security Council (Sanctions Decree People's Republic of Korea 2015) (N.G. 2015, no. 30)
- National Ordinance extension of validity sanction decree 2018 (N.G. 2018, no 34)
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48)

- Central Bank Directives
- Gaming Control Board (GCB) Compliance Measures

❖ **EUROPEAN:**

European anti-money laundering directives (AMLD):

- 4th Directive (EU) 2015/849 of the European Parliament
- 5th Directive (EU) 2018/843 of the European Parliament
- 6th Directive (EU) 2018/1673 of the European Parliament

❖ **INTERNATIONAL:**

- FATF Guidelines on the Risk-Based Approach for Casinos
- FATF Vulnerabilities of Casinos and Gaming Sector

Betrust Entertainment B.V. always applies the strictest regulations and ensures to stay updated to regulatory changes and alerts and recommendations issued by FATF-GAFI, CFATF-GAFIC, and Moneyval.

5. Responsibilities

1. Board of Directors

The Board of Directors is responsible for the development and implementation of Betrust Entertainment B.V.'s compliance framework. The Board of Directors reviews Betrust Entertainment B.V.'s annual risk assessment and compliance report and approves this policy annually.

2. Compliance Officer/Money Laundering Reporting Officer (CO/MLRO)

The CO/MLRO is responsible for developing, implementing, and overseeing all AML, CFT, and KYC procedures, controls, and systems for Betrust Entertainment B.V.'s licensed operations.

The CO/MLRO duties are to:

- To design and implement the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the casino's policy and procedures;
- To organize training sessions for the staff on various compliance-related issues;
- To analyze transactions and verify whether any are subject to reporting according to the

indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;

- To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- To keep records of internally and externally reported unusual transactions;
- To execute closer investigation of unusual transactions if necessary;
- To prepare the external report of unusual transactions;
- To make necessary changes to the AML program;
- To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements; and
- To prepare periodic information on the casino's efforts against money laundering and financing of terrorism and financing of proliferation.

A dedicated 'Suspicious Transactions 'email box has been created which is available to all staff. This mailbox is to be used for all staff to report accounts they suspect of money laundering, especially in the cases if behavioral triggers occur. All such suspicious transactions will be reported internally to the CO/MLRO. Access to this mailbox is restricted to the Money Laundering Reporting Officer.

The CO/MLRO reports directly to the Board of Directors, which in turn has the ultimate responsibility for AML/CFT compliance. The CO/MLRO has access to all Betrust Entertainment B.V.'s data and systems to enable uninterrupted ability to fulfill his or her duties.

6. Risks

The Company operates its business on a Risk Based Approach (RBA). By adopting such RBA the Company ensures that measures to prevent or mitigate money laundering, terrorist financing and proliferation of weapons are commensurate with the risks identified.

Applying such RBA, the Company has to:

- Assess the risks that ML or TF may occur within its organization beforehand;

Design and implement appropriate policies, procedures and controls to manage and mitigate the identified and assessed risks;

- Monitor and improve the effective operation of these policies, procedures and controls;
- Document their risk assessments, including everything that has been done and the reason for this being done.

The risk assessment considers all relevant risk factors, including player, countries or geographic areas, products and services (types of games of chance) that are offered and delivery channels before

determining what the level of overall risk is.

In implementing a RBA, different risk assessments are to be conducted.

ANNUAL BUSINESS RISK ASSESSMENT

The annual risk assessment is conducted to assess the effectiveness of Betrust Entertainment B.V.'s AML controls and systems. The CO/MLRO is responsible for ensuring that the assessment is carried out on an annual basis.

The purpose of the risk assessment is to:

- Identify gaps or opportunities for improvement in the AML policies, procedures, processes, and systems.
- Assess and make informed decisions about Betrust Entertainment B.V.'s risk appetite and implementation of adequate controls.
- Assess allocation of resources and technology for AML/CFT purposes;
- Develop risk mitigation strategies.
- Ensure the Board of Directors and senior management are aware of risks, gaps, and remediation efforts.
- Assist the Board of Directors and senior management with strategic decisions in relation to AML/CFT.
- Assist the Board of Directors with ensuring that resources and priorities are aligned with their risks.
- Ensure that the regulator is made aware of the risks, gaps, and remediation efforts.

Furthermore, employees working in the remote gaming industry are required to make a report in respect of information that comes to them during their business when they have reasonable grounds for knowing or suspecting that a payer is engaged in money laundering or terrorism financing, including criminal spending. The obligations are collectively referred to as grounds for knowledge or suspicion. What the authorities are looking for is what we are able to demonstrate, with supporting evidence, that a risk assessment is and has been undertaken prior to entering into business relationships with customers and that adequate customer due diligence is conducted in order to ensure that the customer's transactions are consistent with the level of risk presented.

CUSTOMER RISK ASSESSMENT(CRA)

A CRA has to be carried out either prior to the carrying out of an occasional transaction, or during the establishing of the business relationship. The CRA will assess the risk the Company's operation will be exposed to when providing services or products to players. When performing a risk assessment of a player, we consider the following indicators:

- Customer Risk

Customer risk is the risk of ML/TF that arises from maintaining relations with a given person. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. Categories of customers whose activities may indicate a higher risk include:

- Customers who have multiple sources of income;
- Customers with irregular income streams;
- PEPs;
- High spenders (money can be derived from illegal activities);
- Disproportionate spenders (inconsistent with casino's information about customer's known source of income/assets);
- Casual customers like locals/tourists, especially when spending pattern changes;
- Improper use of third parties, criminals use third parties to gamble to break up large amount of cash, to buy chips or to cash out on behalf of others to avoid CDD measures;
- Multiple casino player rating accounts to hinder a casino to track their gambling activities;
- Unknown customers (redeeming large amounts of chips);
- Junkets (junket operators monitor player activity and issues and collect credit).

- Product, Service and Transaction Risk

Some products or services are inherently riskier than others and are therefore more attractive to criminals. These include products or services which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the customer to influence the outcome of a game, be it individually or in collusion with others. The use by customers and the acceptance by casinos of specific payment methods, which are considered to present a higher risk of ML/FT, should also be treated as high risk factors. These include:

- Proceeds of crime. Risk that money transferred is derived from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking and theft from the employer;
- Anonymous payment methods such as pre-paid cards and virtual assets;
- Use of casino accounts. This should only be done for gambling purposes and not to deposit and withdraw without gambling or minimal play;
- Types of specific games (e.g. roulette, craps → even bets);
- Peer-to-peer gaming;

- The use by customer of accounts held or cards issued in the name of third parties;
- Multiple casino accounts or wallets (internet operator may own and control multiple web sites);
- Changes to financial institution accounts to fund casino account;
- Identity fraud. Details of financial institution accounts stolen and used on web sites. Also stolen identities used to successfully open financial institutions accounts, and such accounts used on web sites;
- Using cash to fund a pre-paid card poses similar risks as cash;
- Electronic wallets (e- wallets). Not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits. Also, e-wallets which only accept money from financial institution accounts; the financial institution issued statements may only record the payment to the e-wallet, not the transaction to the Internet casino. This may be useful for dishonest customers who wish to disguise their gambling.

- Suspicious Transactions - Behavioral Triggers.

It should be noted that suspicious behavior triggers a further investigation. At all times the customer should be treated with courtesy and where possible, the customer should be kept unaware of any investigations.

In cases of financial risk or suspected fraud, the Risk Department will take appropriate steps to protect funds.

This list below provides examples of suspicious behavioral patterns that trigger further investigation. There is a constant review of behavioral patterns.

- Large amounts of money (from 5.000 euros) deposited within 48 hours of account opening; please specified large amounts
- Large deposits (from 2000 euros), little activity, withdrawal requested to a different method than deposit; please specified large deposits
- Deposit amounts are out of the 'Norm' when compared to the demographic profile;
- Focus purely on multiplayer games, or dual-player games and only with the same people within a 24 hour period;
- Withdrawal Bank Account used by other Accounts;
- Claimed address country differs from IP trace.
- Withdrawal requested to name / address / personal details which differ from registration details;
- The customer has deposited and played during relatively short period of time considerable amounts (more than 20 000 euros per month);
- The person requests that written confirmation will be issued to third party for the prizes won;
- The person pays deposit with the credit card issued to the governmental authority or other similar authority or with the card, which is not linked to any natural person;

- The person requests, after short period of playing for the remaining deposit (more than 2000 euros), to be paid out and requests also confirmation letter for the pay-out;

- Geographical Risk

The geographical risk is the risk posed to the casino by the geographical location of the player and the source of wealth of the business relationship. The nationality, residence and place of birth of the player have to be taken into account as these might be indicative of a heightened geographical risk. Countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction and countries which are known to have terrorist organizations operating are to be considered as high risk. It is advisable to take into account a variety of sources of information produced by the FATF and non-governmental well-known bodies. Some sources to use are:

- Countries on the FATF list of High - Risk Jurisdictions subject to a Call for Action;
- Countries on the FATF list of Jurisdictions under Increased Monitoring;
- Countries on the CFATF Public Statement;
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);
- Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;
- Countries sanctioned by the OFAC;
- Countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International
- Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;
- Countries sanctioned by the OFAC;
- Countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International.

7. Know Your Customer (Customer Due Diligence)

It is prohibited to maintain anonymous accounts or accounts in obviously fictitious names. All customers must be identified. A sound CDD program is the best way to prevent ML, TF and FP. CDD is performed not only as basis for client acceptance, but also on an ongoing basis during the business relationship with the client/customer. The customer risk profile is essential to allow the company's operation /casino to apply a certain level of CDD commensurate to the identified ML/TF risk. And enables the company to assess the customer's behavior within the framework of

the business relationship. This assessment is necessary in order to detect deviations from the expected behavior of the customer. Any deviations, or unusual behavior that is not cleared or motivated accordingly will need to be reported to the FIU via the GoAML portal Curacao.

CDD is divided into two levels:

1. Basic Customer Due Diligence (BDD)
2. Enhanced Due Diligence (EDD)

1. **Basic CDD**

Basic CDD is applicable to all customers.

- Personal details verification:

- Picture/Scan of Government issued ID
- Picture/Scan of Proof of Address

- Financial details verification:

- Picture/Scan of Bank cards used on the site
- Screenshots of e-Wallet accounts or Virtual cards
- Picture/Scan of Bank statements or letter.

- Social network Crosschecking:

- If available, crosscheck the customer's social network information.

7.2 ID

There are 3 different documents accepted as an Identity verification document:

- Picture/Scan of government-issued Identity Card with Picture, expiry date and signature:

- National ID
- Passport
- Driver's License

- Once a document is received it should meet at least the following requirements:

- All 4 corners of the document should be clearly visible.
- All the Information displayed on the document needs to be clearly visible and readable (high resolution).
- The document should not be expired and must be a colored copy.

On the bottom of the document is a machine-readable code that can be checked.

7.3 Proof of Address (PA)

The commonly accepted proof of address is:

- Picture/Scan of Electricity/Water/Gas bill.
- Picture/Scan of Internet Bill.
- Picture/Scan of Landline phone bill (Mobile bill is not accepted).

- Picture/Scan of Letter from the bank or bank statement

Once a document received should also meet the below requirements:

- Full document (All 4 corners visible)
- Clear display of the issuing company, and date of issue of the document
- Clear display of the name and address of the customer.
- Date of issue within the last 3 months.

7.4 Bank Cards

For financial details verification when bank cards have been used requires:

- ❖ Front and back copies of each card used to be provided in accordance with the below requirements:
 - Full document (All 4 corners visible)
 - Of the 16 digits on the front the card; only the first 6 and the last 4 should be visible.
 - The CVV code should be hidden.
 - All the other information should remain visible

5. EDD

EDD is required when a customer and product/service combination is higher in risk and in relation to any transaction that amounts to 2,000 EUR or more, whether the transaction is executed in a single operation or in several transactions that appear to be linked.

EDD shall be carried out if:

- We suspect the customer may be a minor.
- We identify suspicious information provided by players, such as a customer details which are not commensurate with the normal, expected customer profile.
- A customer's total lifetime deposits or withdrawals reach 2,000 EUR.
- A customer is using multiple payment methods.
- A customer has a suspicious deposit pattern, such as name on cards not matching customer's account, high deposit amounts, or high deposit velocity.
- A customer is identified as a PEP.
- A customer qualifies as VIP.
- A customer is from, is resident, or logs in from an IP address in a high-risk country.
- A customer shows any High-Risk Factors (see below).
- We have any suspicion that Betrusted Entertainment B.V. is being used for money laundering or funding of terrorism by the customer or players linked by IP address or other customer data parameters.
- Deposit in one name and pay-out to another name.
- Pass on / sell player account login to another person.
- Deliberately lose funds to the operator.

- Deliberately lose to another player.
- Deposit funds from a bank card flagged as lost or stolen.
- Deposit and leave floating amount or dormant funds in player's account.

In performing EDD, we shall:

- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information on the source of funds or source of wealth of the player. Examples of sources of funds include personal savings, employment, pension releases, share sales and dividends, property sales, gambling winnings, inheritances and gifts and compensation from legal rulings;
- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship.
- Conducting enhanced monitoring of the business relationship;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

It is to be noted that the operation/ casino has the obligation to undertake CDD measures specifically when:

1. Players/customer engage in financial transaction equal to or above EUR2000;
2. Carrying out occasional transactions above the monetary equivalent of EUR2000;
3. There is a suspicion of ML or TF, or;
4. The casino has doubts about the veracity or adequacy of previously obtained customer identification data.

7.6 Failure to Verify a Player's account:

Depending on the case, failure to verify a player's account could lead to one or many of the below actions:

- Freezing of account
- Termination of Account
- Cancellation of bets.

8. Other Due Diligence

1.B2B

B2B partners are generally licensed in reputable jurisdictions to provide gambling products, payment processing, and financial services and are therefore expected to have similar AML/CFT procedures in place to those of Betrust Entertainment B.V.

2.Third-Party Providers

When appropriate, Betrust Entertainment B.V. will carry out corporate due diligence on third party companies that it intends to contract with. CDD may include use of a third-party database to verify CDD information.

3.Ongoing Monitoring

Betrust Entertainment B.V. performs ongoing monitoring on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the company's knowledge of the customer, their spending patterns, gambling preferences, and risk profile, including, where necessary, the source of funds and source of wealth.

If any unusual or suspicious behavior is identified, further investigation is performed in order to determine whether to keep the relationship, request further documentation, terminate the relationship and/or report it to the authorities accordingly.

4. Retrospective

Betrust Entertainment B.V. may by using a risk-based approach decide to do retrospective remediation on existing accounts, where deficiencies are identified or when the company deems necessary.

9. Screening, Training and Awareness Program

Persons working in the operation/ casino operated by Betrust Entertainment B.V. are duly screened prior to entering the workforce for criminal records.

Betrust Entertainment B.V. provides training to all new employees and recurring refresher training for current employees to ensure they are aware of relevant subjects:

- ❖ Anti-Money Laundering and Counter Financing of Terrorism
- ❖ Fraud Prevention
- ❖ Information Security
- ❖ Responsible Gambling
- ❖ All training is managed, administered, and reported on by the MLRO.

The Payments and Customer Services team receives specialized training on monitoring customer registration, payment patterns, gambling activities, and personal information to detect indications of money laundering and respond appropriately to alerts or suspicions of money laundering or terrorist financing activities.

All staff involved with customer accounts and activities on the platform are required to complete a training program to ensure they are fully aware of money laundering indicators and the available reporting structure. This program provides a comprehensive understanding of "normal" patterns and what constitutes suspicious or questionable activity deviating from this norm.

Customer Service Representatives are not required, nor trained, to conduct investigative procedures, as their role is customer-centered. Requiring them to investigate customers would create a conflict.

Yearly updates and refresher workshops are provided to existing staff to keep them informed of issues that have arisen and the ways these were resolved.

10. Record Keeping and CIP

A customer identification program (CIP) involves verifying information provided by a customer. Businesses do this by using independent and legal identification documents. CIP is an important process for any business before establishing a business relationship.

As required by data protection legislation and AML/CFT requirements, Betrust Entertainment B.V. keeps records of the procedures applied to establish the identity of our customers and their transactions history, for at least 5 years after the relationship ends. The records are stored electronically.

11. Reporting Suspicious/Unusual Activities

1. Suspicious Activity Report (SAR)

In accordance with the NORUT, indicators have been issued based upon which unusual transactions are filed. Transactions may include intended and or executed transactions. If a transaction falls within the parameters of one of these indicators the employee managing the respective account of the customer is obligated to report this internally to the MLRO. The MLRO will review and investigate the transaction. The MLRO subsequently report this to the registered MLRO situated in Curacao, who will then conduct a final review for further investigation to determine if the reported transaction is deemed unusual and subject for reporting to the FIU via the GoAML portal Curacao. In accordance with article 21 of the NORUT, it is not allowed to inform the customer and or any third party that a report was filed or will be filed. If the customer or thirds party is informed, this is called tipping off and is considered a criminal offence.

Failure to report an unusual transaction, either internally to the ML:RO or externally by the MLRO to the FIU may result in four (4) years imprisonment and or a fine of the maximum amount

of ANG500,000.00

When an employee submits an internal SAR, the MLRO provides an acknowledgment to serve as:

- Evidence that and safeguard for the employee who submitted the SAR that they have fulfilled their legal obligation of reporting any suspicious activity.
- A reminder that tipping off (directly or indirectly informing the customer that a SAR has been filed) is an offence.
- A reminder that if in doubt they should only contact the MLRO with their concerns.

People who submit an internal SAR shall be protected against any threat, hostile action, adverse acts, or discrimination in the workplace.

The Company operation/casino, its directors, officers and employees are protected by law from criminal and civil liability for breach of any restriction on disclosure of information when reporting to the FIU.

The following transactions or intended transactions are deemed unusual:

a. Transactions which in connection with ML or TF are reported to the police or to the Department of Justice;

b. Transactions by or on behalf of a natural person or legal person, a group or an entity, who is named on a list, adopted by virtue of Sanctions National Ordinance;

c. Transactions in the amount of EUR2000 or more, regardless whether the transaction is made on cash, by check or other form or payment, or through electronic or other non-physical means.

This includes, but is not limited to:

1. A cashless transaction in the amount of EUR2000 or more;
2. Accepting or releasing a deposit in the amount of EUR 2000 or more at the request of the customer;
3. Sale to a customer of chips in the amount of EUR2000 or more (chips include , but is not limited to tokens and credits);
4. A cash out in the amount of EUR2000 or more.

All reported unusual transactions (internally or externally) must be registered systematically in a log maintained by the MLRO.

Where a reported unusual transaction is being investigated by the FIU, the FIU may request the company/casino to retain the records for a period longer than the required 5 years ending the relationship.

12. Independent testing to the AML program

The AML compliance program must be monitored and evaluated at least annually by an independent internal audit department or an outside independent party. The testing encompasses the checking of compliance and adequacy of the relevant compliance procedures a.o.”

- evaluation of the casino’s AML, CTF, CFP manual;
- customer file review;
- compliance management;

- performance of transaction testing;
- assessment of training adequacy;
- assessment of compliance with relevant laws and regulations;
- evaluation of the system's ability to identify unusual activity;
- assessment of the adequacy of the record retention system.

The result of the testing must be documented with any deficiencies reported to senior management with the request to take prompt corrective actions.

12. 13. High Risk Factors

1. PEP

Under a risk-based approach, if a customer is identified to be a PEP, the account must be blocked from making payments or placing bets until the MLRO has approved the account. Note that the decision to accept a PEP as a customer is the responsibility of senior management.

The MLRO must be satisfied that the identified PEP does not pose any risk to the company. In assessing the risk, an important factor is the location of the PEP and whether the PEP is from a high-risk jurisdiction. To assist in the assessment and ultimate decision on whether to continue with the relationship, Betrusted Entertainment B.V. uses available third-party databases that allow it to compare the registration details of the customer with information contained on this database.

The Measures applicable for PEPs are:

- Re-verify Personal and Financial details.
- Establish the source of Wealth.
- Obtain a senior Management approval.
- Conduct enhanced ongoing Monitoring of the business relationship.
- Detect and similarly review any linked accounts.

2. PEP Log

Any identified PEP is recorded within the PEP Log, to enable the MLRO to set up regular reviews and monitoring of these customers. This way, the company can identify any relevant changes which might increase the risk of the relationship and change the decision to accept the account. Where, upon review is confirmed that an existing customer becomes a PEP during the term of business relation, all applicable measures relating to PEP must be performed for approval of business continuation.

3. Sanctions

Betrusted Entertainment B.V. will not knowingly engage in any form of business with any person who

is on a relevant international sanction list.

Sanction checks are performed as part of standard EDD or where there is reason to believe that a customer account requires additional checks. If a customer is on a sanction list a report will be sent to the FIU immediately. Betrust Entertainment B.V. will support the FIU if it becomes necessary to freeze, seize, or surrender funds under the control of a person or institution on the sanctions list.

4. Anonymous Accounts

Betrust Entertainment B.V. does not allow anonymous accounts.

5. Duplicate/Multiple/Shared Accounts

Betrust Entertainment B.V. does not allow multiple, joint, or shared accounts. Accounts are personal and may only be used by one person. Accounts may not be shared or traded.

13. 14.Cooperation with Regulators and Law Enforcement

Betrust Entertainment B.V.is fully committed to working with and cooperating fully with the relevant competent authorities and any law enforcement agency as required.

14. Regular Review

This Policy will be reviewed on a regular basis to ensure that all the latest amendments to the money laundering regulations are kept up to date.

This Policy will be reviewed and approved by the management board of Betrust Entertainment B.V.

15. Non-Compliance

It is the responsibility of all employees to comply with this policy. Failure to do so, will be considered gross misconduct and can result in employee dismissal.

16. Player Funds v. Own Funds: Importance of Player Database

All deposits are initially 100% player funds; these are routed to a bank account or equivalent in the operator's name.

If staked and lost, a player's funds become operator funds. If staked and won in accordance with the T&C, a player's account balance belongs to the player.

Player's bank account balance: Operator funds can only be derived from the Player Database records which track all wins, losses, bonuses and relevant adjustments per player.

❖ Internal controls over funds

- Deposits flow to banks should be made via automated processes – online payment gateways which can be audited.
- Wins and bonuses do not result in a movement at bank. They remain “virtual” unless / until withdrawn.
- Liquidity must consider actual and virtual GROSS liabilities to players.
- If a Player deposit/balance/bet over limit, profiling checks should be triggered.
- Withdrawals should be queued by player via a webpage or app command. These wait for operator approval and subject to internal and External rules (i.e. have funds been played? was bonus wagered enough to be withdrawn? Was the bet(s) funded by Credit card? Any connection to fraud rings etc...?).
- Human screening applied to pay-outs by Anti-Fraud team.

-END-

DocuSigned by:  98427330719E4A1...
DocuSigned by:  E9C1A4A3F74E4ED...

Xecutive Corporate Management B.V.
By Corvin Nagtegaal / Lorenza Godett
General Proxy holder / Director
November 25, 2024