



AML/ CFT/ CPF Policy

For the offering of Online Gambling Under Licence From CGB

POL-CU-AML-03

Current Version

Version	V2.0
Version Date	31-07-24
Contributors	Mike De Graaff - BetComply , Stephen - Grayspace

Revised / Proposed Version

Version	V3.0
Version Date	06-05-25
Contributors	Mike De Graaff - BetComply , Stephen - Grayspace
Approved by	NOT APPROVED (DRAFT)

Table of Contents

1. Overview	3
1.1 Introduction	3
1.2 Legal Scope	3
1.3 Definitions and abbreviations	4
2. The Policy	6
2.1 Definition of Money Laundering (ML)	6
2.2 The definition of Terrorism Financing (TF)	6
2.3 The definition of Financing of Proliferation (FP) of weapons	7
2.4 Business risk assessment (BRA)	7
2.4.1 Customer Risk	7
2.4.2 Geographical Risk	7
2.4.3 Product, Service and transaction Risk	9
2.2.4 Distribution channels risk	9
2.2.5 Technological development risk assessment	9
2.5 AML team	10
2.5.1 AML Compliance Officer	10
2.5.2 Independent AML audit function	11
2.5.3 Training for new employees	11
2.5.4 Training for audit staff	11
2.5.5 Training for AML Compliance employees	12
2.5.6 Training for Supervisors and Managers	12
2.5.7 Training for Senior Management and Board of Directors	12
2.5.8 Periodic Refresher Training	12
2.6 Whistle-blowing procedure	13
2.6.1 Investigation and Follow-Up	13
3. Checks on our players	14
3.1 Player Acceptance	14
3.2 Player account	14
3.3 Customer Risk Assessment	15
3.4 Customer Due Diligence	16
3.5 Enhanced Due Diligence	17
3.6 Transaction Monitoring	18
4 Reporting unusual or suspicious transactions	20
4.1 Recognition of unusual transactions	20
4.2 Reporting of unusual transactions	20
4.2.1 Internal disclosure	20
4.2.2 External disclosure	21

4.3 Termination of the business relationship	21
4.4 Tipping Off	21
4.5 Recording-keeping	22

1. Overview

1.1 Introduction

Bull Gaming NV ("The Company/ Rollbit/ us/ our/ we") has developed and put into effect this Anti-Money Laundering, Combating the Financing of Terrorism, and Counter Proliferation financing Policy (hereinafter referred to as the AML Policy) to mitigate the integrity risks associated with providing licensed online gambling services in Curacao.

We seek to offer the highest security to all of our users and customers on Rollbit.com. For that, a five-step account verification is done in order to ensure the identity of our customers. The reason behind this is to prove that the details of the person registered are correct and the deposit methods used are not stolen or being used by someone else, which is to create the general framework for the fight against money laundering. We also take into account that depending on the nationality and origin, the payment method and withdrawal method, different safety measurements must be taken. Rollbit.com also puts reasonable measures in place to control and limit ML risk, including dedicating the appropriate means.

Rollbit.com is committed to high standards of anti-money laundering (AML) according to EU and other international guidelines, compliance, and requires management and employees to enforce these standards in preventing the use of its services for money laundering purposes.

In accordance with the AML legislation, the board of directors of Bull Gaming N.V. is responsible for the prevention of money laundering on Rollbit.com. The AML Policy has received approval from the Company's directors and is aligned with the broader compliance framework governed by the applicable laws and regulations for providing licensed online gambling services in Curacao. Each major change of Rollbit.com AML policy is subject to approval by the managing director of Bull Gaming N.V.

1.2 Legal Scope

The primary legislation regulating the online gambling industry in Curacao is the National Ordinance on Offshore Games of Hazard (Landsverordening buitengaatsse hazardspelen). Additional laws and regulations on which this AML Policy is based consist of:

Laws and regulations	Abbreviation
the National Ordinance Identification for Services (Landsverordening identificatie bij dienstverlening, PB 2017, no. 92, GT);	NOIS
the National Ordinance Reporting Unusual Transactions (Landsverordening melding ongebruikelijke transacties, PB 2017, no. 99, GT);	NORUT
the Sanctions National Ordinance (Sanctielandsverordening, PB 2014, no. 55, GT);	SNO

the Kingdom Sanction Law

KSL

Unless specified, this AML Policy refers to the above legislation as "applicable laws and regulations".

1.3 Definitions and abbreviations

"Gambling interface" the whole of electronic communication with which we offer the licensed games of chance;

"Games of chance by means of distance communication": a game of chance that is organised remotely on the basis of the license;

"Hyperlink" includes an active icon;

"Licensee": the holder of a license granted pursuant to the NOOGH;

"Online Gambling" means any gaming, where any player enters or may enter the game, or takes or may take any step in the game, by means of a telecommunication, the negotiating or receiving of any bet by means of a telecommunication, or any lottery in which any participant acquires or may acquire a chance by means of a telecommunication

"Player": the person who is registered as a player with the licensee;

"Player account": the account held by the licensee in the name of a player with the playing balance of that player, which is used exclusively for the purpose of participating in the licensed games of chance and which can be traced back to the player;

"player interface": the part of the gambling interface accessible to the player after registration;

"Website", means an electronic communication or set of electronic communications which complies with the Hypertext Transfer Protocol and may be accessed and viewed in visible and legible form by any person having ordinary access to the global system of intercommunicating computers known as the Internet.

Definition	Abbreviation
Anti-Money Laundering	AML
Business Risk Assessment	BRA
Caribbean Financial Action Task Force	CFATF
Customer Due Diligence	CDD
Counter Funding of Terrorism	CFT
Customer Risk Assessment	CRA

Enhanced Due Diligence	EDD
Financial Action Task Force	FATF
Financial Intelligence Unit	FIU
Financing of Proliferation	FP
Curaçao Gaming Control Board	GCB
Know Your Customer	KYC
Money Laundering	ML
National Risk Assessment	NRA
Politically Exposed Persons	PEP
Source of Funds	SOF
Source of Wealth	SOW
Terrorism Financing	TF
Unusual Transaction Report	UTR

2. The Policy

2.1 Definition of Money Laundering (ML)

The conversion or transfer of property, especially money, knowing that such property is derived from criminal activity or from taking part in such activity, for the purpose of concealing or disguising the illegal origin of the property or of helping any person who is involved in the commission of such an activity to evade the legal consequences of that person's or company's action;

The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;

The acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from assisting in such an activity;

Participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points before.

Money laundering shall be regarded as such even when the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

2.2 The definition of Terrorism Financing (TF)

Financing of Terrorism is the financing of terrorist acts, of terrorists and terrorist organisations. A terrorist act is an act to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.

The basic difference between financing of terrorism and money laundering is the origin of the funds. Terrorist financing involves funds for an illegal political purpose, but doesn't necessarily come from illicit proceeds. Money Laundering always involves the proceeds of illegal activity. There is a need for terrorists to disguise the link between the legitimate funding sources and the terrorism. Therefore, terrorists can use similar methods as criminal organisations use to launder money. With money laundering the source of the funds is intended to be hidden, whereas with financing of terrorism the end recipient of the funds is intended to be hidden.

2.3 The definition of Financing of Proliferation (FP) of weapons

Financing of proliferation is the provision of funds 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.

2.4 Business risk assessment (BRA)

The BRA estimates the risk of ML/FT posed by the Company's business and customers.

Risk factors to be taken into account are:

2.4.1 Customer Risk

The ML/TF risk arising from maintaining a relationship with a customer is generally based on the person's economic activity and /or source of wealth. Customers who could pose a higher risk, include but are not limited to:

- Customers with multiple sources of income;
- Customers with irregular income;
- PEPs;
- High spenders;
- Disproportionate spenders;
- Casual customers like locals/tourists
- Customers who use third parties improperly;
- Customers with multiple casino player activity;
- Unknown customers;
- Junkets.

2.4.2 Geographical Risk

Indicators of a geographical risk include but are not limited to:

- Geological location of the player;
- Geological location of the source of wealth of the player;
- Nationality;
- Residence;
- Place of birth.

Countries which are to be considered a high ML/TF risk are:

- Countries with 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;
- Countries which are known to have terrorist organizations operating.

The sources of information regarding the geographical risk level include but are not limited to:

- FATF list of High-Risk jurisdictions subject to a Call for Action;
- FATF list of Jurisdictions under Increased Monitoring;
- CFATF public statement;
- INCSR list of jurisdictions of Concern or Primary Concern in the US;
- European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;
- OFAC sanctions list;
- Credible sources regarding the provision by countries of funding or support for terrorist activities or having terrorist organizations operating within them;
- Transparency International's Corruption Perception Index.

The list of countries and their respective risk ratings can be found in "Rollbit - Country List"

2.4.3 Product, Service and Transaction Risk

Product, services and transactions can cause ML/FT risks, where some products or services will be inherently higher risk than others and considered more vulnerable to criminal exploitation. Certain payment methods are also treated as high risk factors.

High risk factors for product, service and transaction risks include, but are not limited to:

- Proceeds of crime;
- Anonymous payment methods such as prepaid cards and virtual assets;
- Use of casino accounts;
- Specific games such as roulette, craps and bets;
- Peer to peer gaming;
- Use of cards and accounts held in the name of a third party;
- Transferring of funds from one gaming account to another;
- Multiple casino accounts/wallets;
- Changes to financial institution accounts to fund casino account;
- Identity fraud;
- Using cash to fund a prepaid card;
- Games involving multiple operators;
- Electronic wallets (e-wallets).

The products and services and payment methods considered high risk:

- Sportsbetting
- Bitcoin payment methods
- Ethereum payment methods
- Litecoin payment methods
- Solana payment methods

-
- Rollbit coin payment methods
 - Ethereum Tokens payment methods
 - Solana Tokens payment methods
 - NFT payment methods
 - Purchasing Crypto payment methods

2.2.4 Distribution channels risk

The risk profile of a business relationship or a transaction can be influenced by the channels through which a business relationship and transactions are carried out, such as:

- Channels where anonymity is favoured;
- Non face to face channels of interaction with the customers;
- Channels of interaction in between the customer and the Company.

2.2.5 Technological development risk assessment

The ML/FT risk assessment will be done whenever:

- A new product is developed;
- A new business practice emerges;
- A new delivery mechanism, becomes available;
- A new or developing technology is used for both new and pre-existing products.

The BRA is reviewed on an annual basis. This update may be undertaken more frequently under the following circumstances:

- in case of a change in regulatory requirements,
- in case of a change to the business profile,
- following feedback from internal or external audits.

The BRA is carried out by the Compliance Officer, they might be assisted by subject matter experts regarding the operator's customer base, products and services. It is reviewed and approved by Senior Management on a yearly basis.

2.5 AML team

2.5.1 AML Compliance Officer

Rollbit.com has assigned an AML Compliance Officer who is responsible for the detection and prevention of money laundering and terrorist financing. The AML Compliance Officer can act fully independently and has full access to all relevant customer and information. The tasks the Compliance Officer is responsible for are among others:

- To design and implement the AML program;

-
- To verify adherence to local laws and regulations regarding the detection and prevention of money laundering and terrorist financing;
 - To review compliance with the casino's policy and procedures;
 - To organise training sessions for the staff on compliance related issues;
 - To analyse transactions and verify whether any are subject to reporting as unusual transactions;
 - To review internally reported unusual transactions for completeness and accuracy with other sources;
 - To keep records of internally and externally reported unusual transactions;
 - To execute closer investigation of unusual transactions when necessary;
 - To prepare the external report of unusual transactions;
 - To make the necessary changes to the AML policy;
 - 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 efforts of the Company against money laundering and financing of terrorism and financing of proliferation.

2.5.2 Independent AML audit function

The company has the AML compliance program monitored and evaluated at least annually by an independent AML auditor. Rollbit.com assures that the independent AML auditor is sufficiently trained and qualified to assess the AML compliance program. The audit will include, among other things:

- An evaluation of the Company's anti-money laundering, counter terrorist financing and counter financing of proliferation manuals;
- Customer's file review;
- Compliance management;
- Performance of transaction testing;
- Assessment of training adequacy;
- Assessment of compliance with applicable laws and regulations;
- Evaluation of the system's competence to identify unusual transactions;
- Interviews with employees who handle transactions and their supervisors;
- A sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- An assessment of the adequacy of the record retention system.

The AML auditor will also assess whether the Company has acted on earlier audit findings and has made the necessary modifications.

The findings of the audit will be documented and reported to the Board of Directors of Rollbit.com and to the AML Compliance Officer with a request to make the modifications and corrections before a certain deadline.

2.5.3 Training for new employees

When a new employee is onboarded who will be handling customers and their transactions, the employee will be given general training regarding money laundering and terrorist financing and the need to be alert and report any unusual transactions to the Compliance Officer. The evolving AML and trends in the gambling industry will be also included in the general training.

2.5.4 Training for audit staff

Training will be given to the employees who are overseeing, monitoring and testing money laundering controls within the Company. Their training includes changes in regulation, money laundering methods, enforcement and their impact on the organisation.

2.5.5 Training for AML Compliance employees

Training will be given to the employees who run the AML program within the Company. Their training is specialised to stay on top of new trends or changes which impact the organisation and the Risk Management Procedures. This training program includes attending conferences and/or AML-specific presentations.

2.5.6 Training for Supervisors and Managers

Training will be given to the employees who have a supervisory role and managers within the Company. Their training covers all aspects of money laundering, terrorist financing policies, procedures and regulations on a high level.

2.5.7 Training for Senior Management and Board of Directors

Training will be given to the employees who have a senior management role and form part of the Board of Directors of the Company. Their training covers the money laundering and terrorist financing risks to stay aware of the reputational risk that money laundering and terrorist financing poses to the Company.

2.5.8 Periodic Refresher Training

The company provides refresher training to ensure that the employees who handle transactions which may be qualified as unusual, remain informed about the evolving AML policy, regulations and best practices in the online gambling sector.

Feedback and Questions

Employees will be encouraged to provide feedback and seek clarification on any AML-related matters during refresher training sessions.

Training record keeping

Rollbit.com maintains records of the following:

- Details on the content of the training programs;
- The names of the employees who the training was given to;
- The date on which the training was provided;
- The results of any testing conducted to measure the employee's understanding of money laundering and terrorist financing requirements; and
- An ongoing training plan.

2.6 Whistle-blowing procedure

The Company recognizes the importance of maintaining a culture of integrity and transparency within the on-line gambling sector. Employees and stakeholders are encouraged to report any concerns or suspicions related to money laundering, terrorist financing, or any other unethical or illegal activities.

A designated and confidential reporting channel will be established to facilitate the reporting of concerns. This channel will be accessible to all employees, contractors, and stakeholders of the Company.

The Company is committed to protecting the identity of whistleblowers and will not tolerate any form of retaliation or victimisation against individuals who report concerns in good faith.

2.6.1 Investigation and Follow-Up

Upon receiving a report through the whistleblowing channel, the Company will conduct a thorough and impartial investigation.

An independent team will be appointed to investigate the reported concern. This team will have the necessary expertise and authority to conduct a comprehensive inquiry.

The Company is committed to providing timely feedback to the whistleblower regarding the outcome of the investigation, as far as confidentiality and legal obligations permit.

Where appropriate and in compliance with legal requirements, the Company will report concerns raised through the whistleblowing mechanism to the relevant regulatory authorities.

The Company will abide by all legal obligations with regard to reporting concerns related to money laundering, terrorist financing, or other unlawful activities.

3. Checks on our players

Anonymous accounts and accounts in obviously fictitious names are prohibited at the Company. Identification of the player is crucial in order to determine the purpose and nature of the business relationship.

3.1 Player Acceptance

Rollbit.com does not accept players who are:

- residents of Curacao;
- under the age of 18;
- an employee or any key person of the company;
- players who have excluded themselves from participation as long as the self-exclusion period is in place.

In addition, Rollbit.com will not accept and will block the users who:

- Do not provide the identification information requested by Rollbit.com;
- Provide fake identification documents;
- Try to use different means to deceive about their location;
- Are from restricted or prohibited jurisdictions; or
- Are subjected to United States, European Union, or other global sanctions or watch lists;
- Are gambling addicts or have mental health issues;
- Its source of funds are originated or exchanged in restricted jurisdictions;

Rollbit.com reserves the right to block and suspend players for any other reasons at its own description.

Players can only play for real money if they have registered successfully as a player.

3.2 Player account

Every player is assigned a unique player account after completing their registration on Rollbit.com. The following main conditions to each player account apply:

- All payment transactions between the licensee and the player are carried out exclusively through the player account;
- Rollbit.com does not grant credit to players directly or indirectly, whether or not via intermediary;
- We do not allow a negative balance on the player's player account;

- We do not allow a player to participate in a game of chance if the balance on the player account is insufficient to cover the wager. We can only deviate from the previous sentence with the prior approval of the GCB;
- We ensure that all players personal data and transactions are processed and stored in a safe and secure manner;
- We ensure that it always has sufficient funds to pay out the prize money;
- We hold a segregated account for player deposits and winnings;
- Where we use intermediaries for player transactions, the transactions must be recorded in the intermediaries account;
- Bets and or wagers are made in the currency announced;
- Real currencies used by us must be tradeable on international markets;
- Virtual currencies used by us must be tradeable on internationally licensed virtual currency exchanges;
- We cannot exchange currencies in a player's account, provided that such exchange does not include instruments for tokenization;
- The prize money is payable in the same currency that was used to play the game.;
- We provide the player at all times with access to the necessary information relating to the player account and the changes to the player account. This information shall in any case include:
 - a. the current balance of the player account;
 - b. the opening balance of the player account at the most recent login;
 - c. the total stake since the most recent login;
 - d. the total profits and the total losses since the most recent login;
 - e. an overview of all transactions on the player account for a period of at least the last 90 days;
 - f. within how much time after the end of the game the prize money will be available;
 - and
 - g. for how long the prize money remains available, provided that such a period is not less than 30 months from the date it was awarded.

3.3 Customer Risk Assessment

Rollbit.com has adopted a risk-based approach to enable Rollbit.com to understand the nature and purpose of the user relationship to the Rollbit.com platform in order to develop a customer risk profile. The customer risk profile will be done through a Customer Risk Assessment (CRA).

At the first stage, a provisional risk rating will be assigned based on the initially collected information. The level of Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) is calculated on the outcome of the CRA.

3.4 Customer Due Diligence

At account opening, Rollbit.com collects documentary and non-documentary information:

- Collecting baseline (e.g., wallet address, email address) information at account creation through Rollbit.com's user onboarding portal;
- Monitoring the risk profile associated with the underlying cryptocurrency wallet used to fund the user's account;
- Maintaining records of the information used to identify the user; and
- Determining if a user appears on any list of known or suspected terrorists or terrorist organisations provided to the financial institutions based on the above information.

The above steps are operationalized using the following measures:

- **Identity and Age Verification:** the following information will be at a minimum collected for identification of the player:
 - Full name;
 - Permanent residential address;
 - Date of birth;
 - Place of birth;
 - Nationality; and
 - Identity number.

* For a low risk player profile, the full name, permanent residential address and date of birth is sufficient.

*For high risk players, the above mentioned information might not suffice and the need to request additional information arises.

A third-party service provider will support Rollbit.com's ability to determine the legitimacy of the identification information other KYC materials or information provided and will confirm that the user is permissible. The service provider also will confirm that the user does not appear to be located in a comprehensively sanctioned or otherwise prohibited jurisdiction and will search global sanctions lists to confirm that the user does not appear thereon using onboarding information such as wallet addresses.

- **Customer Information:** Rollbit.com will collect details on each user to form a reasonable belief that Rollbit.com knows the identity of its users commensurate with the user's risk profile. For instance, Rollbit.com may collect such details as the wallet address, name, address, country, date of birth, or postal code (collectively, "KYC Information").
- **Beneficial ownership:** Rollbit.com will take all necessary measures to verify the identity of the beneficial owner(s) for all persons holding 25% or more of the shares or voting rights and for any person who exercises the ultimate effective control of the customer. This will go as far as understanding the ownership and control

structure of the customer in case of legal persons and legal arrangements. The obtained information and data need to be coming from a reliable source to be able to successfully verify the identity of the beneficial owner(s).

CDD will be performed at any time when:

- Customers engage in financial transactions equal to or above NAf. 4,000;
- There is a suspicion of money laundering or terrorist financing; or
- The casino has doubts about the veracity or adequacy of previously obtained customer identification data.

A transaction can be a single transaction or a series of transactions, leading to the equal amount of NAf. 4,000 or above.

If the requested information and documentation is not received within 30 days from the moment the NAf. 4,000 threshold was met, the Company will terminate the relationship with the customer and report the transaction to the FIU.

3.5 Enhanced Due Diligence

High risk customers will undergo a Enhanced Due Diligence to determine whether their behaviour and transactions are unusual and need to be acted on accordingly.

In any case, EDD will be conducted where the ML/TF risks are higher, such as:

- Residents of higher risk geographic areas;
- PEP's
- Product or transactions that might favour anonymity;
- New products and new business practices and the use of new or developing technologies for both new and pre-existing products.

Rollbit.com performs ongoing monitoring on its users in order to detect any behaviours or indicators that might raise suspicions in regard to money laundering and terrorism financing practices. For that purpose, Rollbit.com has implemented a set of red flag indicators that help it determine such behaviours and require further action from Rollbit.com in assessing the customer information.

Whenever one of those red flags is triggered, the user account will be suspended and Rollbit.com will pursue enhanced due diligence. Enhanced due diligence under this policy is deemed to include, but not limit to, the provision of:

- Full legal name;
- Country of citizenship;
- Permanent Address (which, for an individual, must be a residential or business street address, and for an entity, must be a principal place of business, local office or other physical location);
- Identification number (either a taxpayer identification number, or, if unavailable, a passport number and country of issuance, alien identification card number or number and country of issuance of another government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard);

-
- Identification Document;
 - Reason for intended or performed transactions;
 - Source of Funds and Source of Wealth.

Rollbit.com may use third-party service providers to verify any of the above information as determined to establish a reasonable basis to know the true identity of the user where the user's activity warrants such action.

The approval of senior management of Rollbit.com is needed to decide on any change in the business relationship.

3.6 Transaction Monitoring

Rollbit.com will conduct ongoing monitoring on a regular basis using rule-based systems developed in-house and others from third-party vendors to review user history and patterns of activity to detect and report any unusual activity as required and to develop and implement any additional controls or limits in its platform.

Rollbit.com has implemented procedures addressing the following two key components of unusual or suspicious activity:

- Identification of unusual activity through methods of identification may include employee and customer identification, law enforcement inquiries, other referrals, or transaction and surveillance monitoring system reports; and
- Alert management that focuses on processes used to investigate, evaluate and document identified unusual or potentially suspicious activity.

Rollbit.com will use the following processes to achieve both goals:

- **Transaction Monitoring for Sanctioned or Prohibited Jurisdictions:** Rollbit.com may in its reasonable discretion impose certain due diligence requests at user balance withdrawal. Rollbit.com presently conducts a mixture of manual and automated transaction monitoring processes to identify "red flag" behaviour. Where such red flag behaviour is identified, Rollbit.com may refuse to process any withdrawal attempts or collect additional information from the recipient. Rollbit.com will further endeavour to limit any attempted user account funding from prohibited jurisdictions (which are identified in the Rollbit.com user-facing disclosures and updated from time to time internally) where the associated wallet address indicates that the user or the user's funds are located in such a prohibited jurisdiction. For instance, Rollbit.com may prohibit a user from funding their Rollbit.com account using a known U.S. based exchange wallet as such assets indicate that the user is a U.S. person. Users will have the ability to rebut any suspension with additional information as part of Rollbit.com's ongoing transaction monitoring and user due diligence standards.
- **Screening for Sanctioned Parties:** Prior to issuing a Rollbit.com funding address to a user, Rollbit.com will screen a user's wallet address against applicable sanctions databases. Such screening measures will rely on third-party blockchain forensics vendors such as Chainalysis. Rollbit.com will periodically re-screen wallet addresses against such databases.

- **PEP screening:** Prior to engaging in a business relationship with a customer and before any transaction is made, the customer will undergo a PEP check. Any family member or close associates to the PEP customer will also be assigned a PEP status and will be treated equally as a PEP. As with any new customer, the PEP will undergo a Customer Risk Assessment, where the following will be taken in consideration:
 - The type of public function of the PEP;
 - The country from which the PEP originates;
 - The transactions that the PEP carries out.

Depending on the outcome of the Risk Assessment, the PEP may or may not be able to play. The approval to service the PEP to establish the business relationship, maintain the business relationship or any transaction done by the PEP, will be obtained by senior management or the Compliance Manager.

In any case, a PEP customer will request a statement regarding the Source of Wealth (SOW) and Source of Funds (SOF) which will be verified.

PEP's will be ongoingly monitored during the business relationship.

- **Identification of Unusual Activity:** Rollbit.com will monitor account activity for unusual size, volume, pattern, or type of transactions, taking into account risk factors and red flags that are appropriate to its business. Monitoring will be conducted running regular reports of unusual, high risk, or suspicious user activity. If any transaction is seen as unusual and needs to be reported, Rollbit.com files a Unusual Transactions Report (UTR) to the FIU.
- **Anti-Mixing Measures:** Rollbit.com will utilise software designed to detect other suspicious deposit or withdrawal patterns. Such instances will be dealt with on a case-by-case basis, depending on the perceived level of risk. In such instances, a user may be required to explain their methodology and purpose for using the platform.
- **Chainalysis Review.** Every single crypto deposit or withdrawal both indirect and direct will run through Chainalysis and be reviewed for signs of fraud or suspicious behaviour. A user's account will be suspended and reviewed upon alert of potential illicit behaviour. Sufficient proof of wealth may be requested from high-risk accounts. Rollbit.com may refuse to withdraw to certain "high-risk" addresses as determined in consultation with Chainalysis risk scoring.
- **Withdrawal Threshold KYC:** Additionally, and independently, every account, wherever or with whomever associated, will be suspended until adequate KYC diligence occurs once that account reaches a withdrawal threshold dependent on the account's risk characterization over the life of the account.

4 Reporting unusual or suspicious transactions

The Company is committed to promptly identifying and reporting any suspicious activities related to money laundering, terrorist financing, or any other unlawful activities within the online gambling sector to the Financial Intelligence Unit (FIU).

4.1 Recognition of unusual transactions

An unusual transaction is a transaction inconsistent with the player's profile. Therefore, it is important to know the customer and understand the player's risk profile for the Company. Transactions can have objective and subjective indicators to lead to the determination of the transaction being unusual and the need to file a report.

The following transactions are seen as unusual:

- Transactions which are reported to the Police or the Department of Justice, in relation to money laundering or terrorism financing;
- Transactions by or on behalf of a natural person or legal person, a group or entity, named on a Sanctions list;
- Transactions in the amount of NAf. 5,000 or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non-physical means. This can be:
 - A cashless transaction in the amount of NAf. 5,000 or more;
 - Accepting or releasing a deposit in the amount of NAf. 5,000 or more at the request of the client;
 - Sale to a customer of chips (a.o. tokens and credits) in the amount of NAf. 5,000 or more;
 - A cash out in the amount of NAf. 5,000 or more.
- Transactions where there is cause to presume money laundering transactions or terrorist financing.

A transaction may be a single transaction or a series of transactions leading to the total amount of NAf. 5,000 or more.

4.2 Reporting of unusual transactions

All employees are trained to recognize unusual transactions and are obligated to be vigilant and promptly report to the Compliance Officer any transactions or behaviours that raise suspicion in accordance with the NORUT.

Any intended or actual unusual transaction will be reported to the FIU with no delay.

4.2.1 Internal disclosure

All employees can file suspicious activity reports in one of the following ways:

1. Via email to legal@rollbit.com
2. Anonymously via a letter to Abraham de Veerstraat 9 in Curaçao

Though employees are encouraged to file suspicion via email, as that enables us to ask follow up questions or request more information to the reporter, employees are in liberty of filing suspicious activity anonymously.

All internal disclosure should be raised without undue delay. Once received, the employee will receive an acknowledgement receipt of the internal disclosure.

4.2.2 External disclosure

The Company acknowledges its legal obligations to report unusual transactions to the authorities. Unusual transactions reports (UTR) will be filed to the FIU through the goAML reporting portal in the English language.

When reporting to the FIU, all directors, officers and employees of Rollbit.com are protected by law from criminal and civil liability for breach of any restriction on disclosure of information.

A detailed record of all UTR files, including supporting documentation and correspondence with the authorities, will be maintained to demonstrate compliance with reporting obligations.

4.3 Termination of the business relationship

In case the obligations rising from the CDD or EDD can not be met, Rollbit.com will not establish a business relationship with the customer or perform a transaction. In some cases, Rollbit.com will decide to terminate the business relationship with the customer.

Depending on the outcome of the CRA and the CDD or EDD, the customer's account will be either blocked or closed.

Rollbit.com will use the information and all factors in relation to this customer, to determine whether or not there are suspicions of ML/TF/FP. In that case, a UTR will be filed at the FIU. In case the customer's account is closed and there is no reason to retain the funds of the customer, the funds will be paid back to the customer, using the same channels used to receive the funds.

4.4 Tipping Off

Tipping off occurs when each of the following criteria are met

- The employee discloses either that a suspicious activity report has been/will be made. Or an investigation is being/or is likely to be made; and
- The employee knew the information through their work in the regulated sector.

It is a criminal offence which aims to stop staff members giving the “heads-up” to customers that are suspected of criminal activities as this could prompt them to move criminal/terrorist funds, destroy evidence or evade arrest.

As a consequence, the requirement to conduct EDD in the event of suspicious activity is disapproved where there is concern that it may tip off the customer and only an unusual transactions report (UTR) will be filed to the FIU.

4.5 Recording-keeping

The Company will maintain comprehensive records related to customer due diligence, transactional activities, and any other relevant documentation.

Records will be retained for a minimum period of 5 years after the business relationship is ended or after the transaction date.

The records will be easily accessible to authorised personnel and relevant regulatory authorities for inspection or audit purposes.