



AML/CFT Policy

OVERVIEW

The company adheres to strict codes of conduct in order to protect the company's good standing, instill trust with the customers, comply with regulatory requirements and fulfil its ethical responsibility. The company warrants that it will:

- Verify players prior to establishing a business relationship
- Deal only with players who have registered an account
- Comply with regulatory requirements and industry best practice
- Do its utmost to ensure that no funds are accepted which originate from illegal activities
- Prevent all cases when its Services might be used as a tool in Money Laundering

1. Table of Contents

2. Policy statement	5
3. Introduction	6
3.1. Definition of Money Laundering	6
3.2. Definition of Financing of Terrorism	6
3.3. Definition of Financing of Proliferation	6
4. Laws and Regulations	7
5. The Risk Based Approach	8
5.1. Definition	8
5.2. Risk Assessment	8
5.2.1. Transaction Risk	9
5.2.2. Interface Risk	10
5.2.3. Geographical Risk	10
5.2.4. Player Risk	11
6. Customer Due Diligence (CDD)	12
6.1. Threshold for Customer Due Diligence	12
6.2. Customer risk assessment	12
6.3. Identification and Verification of the Customer	13
6.3.1. Verification through documentary sources	14
6.3.2. Electronic means	15
6.4. Enhanced Due Diligence	15
6.5. Timeline for Compliance and Non-Compliant Documents	16
6.6. Ongoing player monitoring	17
6.7. Ongoing transaction monitoring	19
6.8. Termination of business relationship	19
6.9. Ultimate Beneficial Owner (UBO) Identification and Verification	20
6.10. Business Affiliate and Supplier Diligence	21
7. Reporting of unusual transactions and activities	21
7.1. Appointment of the Compliance Officer (CO)	21
7.2. What is unusual activity?	22
7.3. How to Report unusual transactions and activities	23
7.3.1. Internal Reporting Procedures	23
7.3.2. External Reporting Procedures	24
7.3.3. Reporting Timelines	25
7.3.4. Stopping/continuing work following a suspicion	25
7.3.5. Disclosure	25
7.4. Curacao Financial Intelligence Unit	26
8. Payout Management Procedure	26
9. Employee Screening and Training	28

10.	<i>Independent Audit Function</i>	<i>31</i>
11.	<i>Keeping records of client due diligence information.....</i>	<i>32</i>
11.1.	Internal Procedure for Submitting a UTR.....	32
11.2.	Examples of Unusual Transactions	33
12.	<i>Appendix 1: Unusual Transaction User Report Template.....</i>	<i>34</i>
13.	<i>Appendix 2: Country Risk List</i>	<i>38</i>

Version	2.1				
Date Created	19.12.2025				
Author(s) of Document	Compliance department (NC)				
Purpose of Document	The document defines: • How the company goes about minimizing its exposure to Fraud • How it identifies its customers What measures are taken to limit the company's exposure to Money Laundering and the reporting requirements in this regard how settlements towards players are carried out.				
Security Class	Confidential				
Authorized by	Gouloud Hammoud obo Guardian Corporation Curacao B.V.				
REVISION HISTORY					
Version	Date of Issue	Author	Security Class	Changes	Approved By
1.0	05.04.22		Confidential	Initial Release	Plexian Network B.V.
2.0	28.01.25	Compliance Officer	Confidential	Alignment with GCB AML Regulations	Plexian Network B.V.
2.1	19.12.25		Confidential	Updates following GCB review	Plexian Network B.V.

Approved By:	Guardian Corporation Curaçao BV obo Plexian Network BV represented by: G. Hammoud Corporate Director
Signature:	
Date:	19 December 2025

2. Policy statement

It is the policy of Plexian Network B.V. (hereinunder referred to as 'the company') that all members of staff shall actively participate in preventing the services of the company from being exploited by criminals and terrorists globally for purposes of money laundering or used to fund terrorist activity through winnings obtained through wagering on the company's website or by trying to move money around by using multiple cards or payment methods. We have a zero-tolerance approach to Money Laundering, Funding of Terrorism, and other financial crimes.

This policy sets out procedures to allow our staff to understand and be confident in reporting on any unusual transactions or activity to the Compliance Officer (CO) within the company. A big part of this is how we educate and train our staff. This document will outline how we do this, what is considered and how its implemented in our day-to-day operations.

Objectives of the policy:

- Ensuring the company's compliance with all applicable laws, statutory instruments of regulation, and requirements of the relevant supervisory body
- protecting the company and all its staff, as individuals, from the risks associated with breaches of the law, regulations and supervisory requirements
- preserving the good name of Plexian Network B.V. against the risk of reputational damage presented by implication in money laundering and terrorist financing activities
- making a positive contribution to the fight against crime and terrorism.

In order to achieve these objectives, it is company policy that:

- every member of staff shall meet their personal obligations as appropriate to their role and position within the company,
- commercial considerations shall never be permitted to take precedence over Plexian Network B.V.'s anti-money laundering commitments,
- the company shall appoint a Compliance Officer (CO) to ensure continuation during his / her absence, and they shall be afforded every assistance and cooperation by all members of staff in carrying out the duties of their appointments.

3. Introduction

Plexian Network B.V. believes that prior to implementing its Fraud Management Procedures, it is essential for it to identify what constitutes money laundering and funding of terrorism first.

3.1. Definition of Money Laundering

Money laundering (ML) is the movement or concealment of criminal proceeds, with the aim of obscuring the link between crime and the generated funds through the placement, layering and integration stages of ML, so as to be able to ultimately avail oneself of the profits of crime. During the initial stage, the funds are placed into the financial system, which in the case of the company would be through the player deposits. The next stage would be the layering stage, whereby involving a complex system of transactions designated to hide the source of the funds, for example involving players betting through multiple accounts. The integration stage would appear at the final stages through the customer's withdrawal of the funds, making the funds appear to have originated from a legitimate source. Hence, the ultimate aim of ML is obscuring that the original source of funds is criminal activity.

3.2. Definition of Financing of Terrorism

Funding of terrorism on the other hand is the process of making funds or other assets available, directly or indirectly, to terrorist groups or individual terrorists to support them in their operations. This may take place through funds deriving from legitimate sources or from a combination of lawful and unlawful sources. Indeed, funding from legal sources is a key difference between terrorist organizations and traditional criminal organizations involved in money laundering operations.

Although it would seem logical that funding from legitimate sources would not need to be laundered, there is nevertheless often a need for terrorists to obscure or disguise links between the organization or the individual terrorist and its or his legitimate funding sources. Therefore, funding of terrorism is mostly concerned with obscuring the end recipient of the funds. Terrorist financing is a serious threat to financial businesses or businesses involving a high level of monetary transactions, such as within the gaming industry.

3.3. Definition of Financing of Proliferation

Financing of proliferation (PF) 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.

4. Laws and Regulations

The authorities in charge of the supervision of AML, CTF and CPF matters for the gaming sector are the Curaçao Gaming Control Board (GCB) and the Curaçao Financial Intelligence Unit (FIU). The following laws and regulations, as well as any additional regulations issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law, are applicable to the Company:

- Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6.;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- National Decree for general measures, of the 10 July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10 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 United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30);
- 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 United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- Curaçao Gaming Control Board Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025.

As a member of the Financial Action Task Force (www.fatf-gafi.org) and of the Caribbean Financial Action Task Force (www.cfatf-gafic.org), Curaçao is meeting international standards by regularly implementing the core standards of these organizations in its national legislation.

5. The Risk Based Approach

5.1. Definition

As per the applicable laws, Plexian Network B.V. adopts a risk-based approach. It hence identifies and analyses its risks and subsequently makes use of measures, policies, controls and procedures to curb any undesired risks, amongst which those related to the money laundering and funding of terrorism risks from materializing. The approach allows for flexibility and significant discretion to be exercised by Plexian Network B.V. This entails significant responsibility. It is up to Plexian Network B.V. to show via adequate documentation, including but not limited to a risk analysis process, that it has assessed all risks and adequately put into place any measures to control these risks. In this regard this policy lays out the specific steps which Plexian Network B.V. will adopt to ensure that its conduct is in line with the Risk Based Approach in respect of considering and identifying those risks that directly impinge on money laundering and funding of terrorism.

5.2. Risk Assessment

The Business Risk Assessment (BRA) framework is a crucial component of Plexian Network B.V.'s AML, CTF, and CPF compliance program. It provides a systematic, risk-based approach for identifying, assessing, and mitigating money laundering, terrorist financing, and proliferation financing risks within the Company's operations.

Plexian Network B.V. performs thorough BRAs, evaluating potential risk factors related to customers, products, services, geographic locations, and delivery channels. Each risk factor is assessed for its likelihood and potential impact using both quantitative and qualitative data. Tailored controls and measures are then implemented to address these risks. All findings, evaluations, and mitigation strategies are documented and reported to senior management and relevant regulatory authorities.

Risk Management entails:

- i) recognition of existence of risk;
- ii) undertaking of a risk assessment, and
- iii) implementing systems and strategies to manage and control the identified risks.

There is no doubt that the business of remote gaming is deemed risky. The risk assessment will however identify the key risks the company faces as well as the level of these risks, so that, consequently, the necessary measures are adopted to manage and control the identified risks. This procedure will specify the controls and processes that are to be followed so as to ensure that the risks which Plexian Network B.V. has identified and which it will face as part of its operations will not materialize.

The Business Risk Assessment (BRA) shall be formally reviewed at least annually and whenever material changes occur to the Company's business model, products, payment methods, geographic exposure, or regulatory environment.

The BRA, including the Company's risk appetite and key risk mitigation measures, shall be submitted to the Board of Directors for formal approval. Evidence of Board review and approval shall be documented and retained.

The Compliance Officer is responsible for coordinating the annual review of the BRA and ensuring that any identified changes in risk are reflected in the Company's policies, procedures, and operational controls.

Plexian Network B.V.'s organizational risk assessment takes the following factors into consideration:

5.2.1. Transaction Risk

Some gaming products/services/transactions are more vulnerable to criminal exploitation than others. These include, for instance, gaming products or services that allow the player to influence the outcome of a game, be it one player alone or in collusion with others.

Transactional Risk Matrix:

- Transfer of Funds - Transfer of funds between players is not permitted and there is no facility that would enable the players to do so.
- Multiple Source of funds - Usage of multiple payment methods at any one time represents a high risk. Hard coded restrictions and limitations are currently in place to ensure risk exposure is minimized at any given point in time.
- Multiple accounts - Internal controls are in place to limit and hinder players from opening multiple accounts under the same brands.
- Shared Platforms/Games involving multiple operators - While the company makes use of B2B game providers/platforms which are used by other operators there is no possibility of players transacting with each other across platforms. Peer 2 peer gaming is not offered by our company, fully mitigating such risk such as chip dumping.

Payment method risk Matrix

Deposit/ Withdrawal Methods	Low	Low-Medium	Medium	Medium - High	High
Bank Transfer	X				
Bank Issued Debit and Credit Cards		X			

Debit and Credit Cards issued by other licensed financial institutions		X			
Electronic Wallets and Virtual Currencies			X		
Crypto					X
Prepaid cards/ vouchers					X
Peer to peer transfers (Not Available)					X
Interac	X				

5.2.2. Interface Risk

Plexian Network B.V. establishes a business relationship and/or through which transactions are carried out. No presence transactions, which is common in our industry, are no longer considered as automatically high risk, as long as technological measures and controls are in place to address the risks like risk of identity fraud or impersonation. Plexian Network B.V. offers a smart combination of verification methods based on both documentary and electronic sources as mentioned below, to counter the mentioned risks. For instance, though Plexian Network B.V. will make use of electronic databases, it is well aware that the databases only confirm that the identification details provided correspond to those of an actual person, and not that the player is actually that individual. Provision of additional identification documents will provide further proof that Plexian Network B.V. was justified in considering that the player is actually the person he alleges to be.

5.2.3. Geographical Risk

Plexian Network B.V. has, depending on the geographical region, risks as well however also the geographical locations of its suppliers and service providers. The element to be considered in respect of this fraud management procedure is primarily attributable to the players and the source of funds of the said customers. The entered country and/or IP address of a player is taken into consideration as these might be indicative of a heightened geographical risk in their area. Countries that have a weak anti-money laundering and counterfeit terrorism system, countries known to suffer from a significant level of corruption, and countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction will be considered as high risk. The opposite is also true and why the company may be considered as presenting a medium or low risk. Plexian Network B.V. services use

information on MaxMind when making a decision regarding the geographical risk of each registered customer. The Basel AML Index and the FATF High Risk and Other Monitored Jurisdictions publications may also be considered when assessing geographical risk.

Risk assessments are 'works in progress', constant throughout the life of the player with the company. Such assessments are to be constantly re-evaluated as new risks emerge and as time goes by. Risks may emerge due to changes in technology, which may render money laundering, or the funding of terrorism attempts easier to carry out. Other changes include widening of the customer base or the addition of games and payment methods which present a different risk profile from those already offered. In determining the level of risk posed by a customer, the accumulation of all the relevant indicators will be taken into consideration. These together determine the player's risk profile contributing to the totality of a player's risk profile.

5.2.4. *Player Risk*

The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. In identifying the level of risk inherent in a relationship, Plexian Network B.V. will be assessing what would be the likelihood that a player would be able to launder proceeds of crime through Plexian Network B.V.'s service. A high earning player who spends a fourth of his monthly wage in wagering is not likely to constitute a high risk, even if the amount being wagered is large. On the other hand, a minimum wage earner who spends his only wage on wagering will more likely constitute a high risk. Furthermore, the individual will be screened to determine whether he is a politically exposed person (PEP), or in any way associated to a PEP, which would be classified as high risk. Checks would also be carried out to ensure that the individual is not subject to any sanctions or other statutory measures.

6. Customer Due Diligence (CDD)

6.1. Threshold for Customer Due Diligence

The Fraud Management Procedure will now focus on the getting-to-know the players procedure and identifying the risks related to their transactions and the origination of their funds, both from where the funds were obtained as well as the source of the funds from where the player has remitted the funds.

Plexian Network has an obligation to undertake CDD measures when:

- players engage in financial transactions¹ equal to or above the monetary equivalent of NAf. 4,000.00;
- carrying out occasional transactions above the monetary equivalent of NAf. 4,000.00;
- 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.

6.2. Customer risk assessment

As described above, a risk assessment can never be a one-size-fits-all exercise. Plexian Network B.V. will in this respect carry out a risk assessment upon entering into a business relationship with or carrying out an occasional transaction for a customer. For the purposes of clarity, Plexian Network B.V. will not be accepting corporate players only individual players.

The Customer Risk Assessment (CRA) assesses the particular risks Plexian Network will be exposed to when providing its services or products to customers. The information collected to draw up the CRA will formulate the customer's risk profile. The risk assessment will categorize customers as low, medium, or high risk, with due diligence and ongoing monitoring applied proportionately.

The risk assessment mentioned will allow Plexian Network B.V. to develop a risk profile concerning the player and categorise the risk as low, medium or high, thereby allowing it to identify the controls which need to be adopted. The player's risk profile will not be completed upon registration. The registration part of the process will only signify the start of the collection of information, and as such the risk profile will be increased and refined with the development of the relationship with the player. Having said that, should there be a change in the business relationship entertained with the customer, which therefore also entails a change in the risk identified, the measures adopted to control the risk shall be adapted accordingly. Furthermore, ongoing monitoring, as explained in more detail below, will ensure that any change in risk is spotted as soon as possible. The level of monitoring will be commensurate to the risk

¹ Financial transactions refer specifically to deposits and withdrawals, excluding bonuses. Wagered amounts and winnings fall under gambling transactions, which are not classified as financial transactions. To determine when a player reaches the monetary equivalent of NAf. 4,000 for CDD purposes, the Company will consider not only individual transactions but also any series, combination, or pattern of transactions that exceed this threshold. This calculation will be performed daily and will include all deposits and withdrawals made by the player, as well as any peer-to-peer transfers.

posed by the particular customer, but systems will be put in place so as to detect developing risky situations.

To start off, Plexian Network B.V. adopts CDD measures so as to determine who its players are. All details collected at registration stage are used to build the player profile. Further player profiling is done, based on the customer's activity and also on the particular behavioral aspects. This profiling aspect will assist in determining the risk attached to the particular player and thus also facilitate in the identification of future unusual behavior. CDD is divided into the below three parts:

6.3. Identification and Verification of the Customer

During the identification process players will be requested to submit documentation to the compliance team. This information is collected during the registration process. The personal information to be collected is to start off the Know Your Client (KYC) process, which includes the collection of the following personal details:

- Name and surname
- Permanent residential address
- Date of birth, as the player must be over eighteen years of age (*or legal age as applicable in the player's particular country*)
- Valid email address
- Gender
- Country of Residence

Once the email is validated as current/active and an active email the account is then opened.

Once the above information is provided and the player has successfully created his account, and before making their first deposit, Plexian Network B.V. will first check whether the individual in question is a PEP, a family member of the PEP, or a close business associate of the PEP.

A reliable electronic database, such as Company Advantage, is used. At the same time the team also runs the player through minFraud, riskScore from Maxmind to determine certain risk attributes and perform screening against relevant sanctions lists. The data within the Comply Advantage database which is currently used through our third-party service provider is derived from information on sanctions watch or regulatory and law enforcement lists. And Maxmind helps us by using risk scoring and data to identify high-risk activity in e-commerce payments, platform user activity, incentivized traffic, and more. And also specialize in GeoIP intelligence for compliance, fraud detection, security and more.

Comply Advantage data consists of PEP information as well as information about individuals and entities not found on official lists but who instead are reported to be connected to sanctioned parties or reported to have been investigated for, or convicted of engaging in, financial crime, slavery, and human abuse-related activities (SIP and SIE). Comply Advantage also forms profiles with unfavorable information (risk data) on public and private entities. The information is found in adverse media, or negative news: these are both 'traditional' news outlets, niche media organizations,

government and regulatory press releases, and reliable blogs.

Therefor by using these 3rd party tools we can establish a lot about the player from the very beginning.

If a true match against sanctions hit is confirmed, Plexian Network must immediately proceed with freezing the funds of the particular customer(s) (if applicable), in accordance with the Sanctions Ordinance, and in any casemust immediately file a report with the FIU. Once the true match is confirmed by the supervisory authority, Plexian Network shall terminate services and keep the frozen assets until further instruction from the supervisory authority, or otherwise, in light of tipping off considerations, follow instructions from the supervisory authority.

If it is determined that an individual is a PEP or in any way related to a PEP, then the individual will be deemed himself / herself a PEP and will not be allowed to deposit the money as a player with Usoftgaming N.V. and would be blocked at the deposit level. The account will be followed by permanent closure. This therefore means that determination as to whether an individual is a PEP (as per above definition) will take place after the registration stage, but before the first deposit.

In any situation where the player is immediately identified as being high risk, Plexian Network B.V. may immediately ask for additional personal details and for their verification. In any case, Plexian Network B.V. will ensure that it is always able to determine that the player is who he claims to be and that the measures adopted are effective enough to counteract the risk of identity fraud and impersonation.

For example, the team may request a video call with the player to assure its truly them. And in some cases, has asked the players to visit local registered notaries to get identification documents notarized.

Verification consists in confirming the personal details collected for identification purposes using independent data, information and documentation obtained from reliable sources. If inconsistencies in the personal information provided by the player are identified, Plexian Network B.V. will consider whether to adopt additional identification and verification measures. This will take place by either of two ways:

6.3.1. Verification through documentary sources

Only documents issued by government agencies that include a photograph are deemed reliable for verifying the customer's identity. Documents issued by the government that lack a photograph can be used to confirm the customer's current address, provided the address is included in the document. Plexian Network accepts as proof of permanent residential address copy of utility bill (e.g. electricity, water, gas, telephone landline)² or bank statements, as long as they are not older than 3 months at the time they are received.

If the player's residential address cannot be verified by using any one of the just mentioned documents, Plexian Network B.V. will ask for alternative reliable

² Bills issued for mobile phone services are not acceptable, as they are generally not tied to a fixed location.

documents such as a recent bank statement, Government tax documents or other documents depending on the players situation, to assure we can 100% establish the players' current address.

The documents requested will be received by email and if deemed necessary notarized documents may be requested from time to time.

Plexian Network B.V. will ensure that all documents received are clear and readable documents and are authentic or reflect authentic ones. Some documents, such as passports may be easier to verify as these can be checked against online databases. In other cases, such as with regards to utility bills, the verification process may be less easy to establish but notarized utility is something our team is gravitating too more and more.

In respect of the validity of the information provided, Plexian Network B.V. will also consider other data that is collected from the player such as geo-location, IP address data via MaxMind, that should under normal circumstances back up the data obtained in the documents provided by the player.

There will be exceptions, where the IP address will not tally with the country / location, this is something our team is aware of and specialize in. Such instances need to be checked on a case-by-case basis and during verification some questions will be asked to the player for clarification.

6.3.2. *Electronic means*

Sources like E-ID or Bank-ID and electronic commercial databases are used as well. Plexian Network B.V. is well aware that the reliability of these databases may not always be the most accurate. In this regard it will consider what source of information is feeding into the database and whether such data is generally known to be maintained or accurate.

When using electronic databases, Plexian Network B.V. will also make use of other documentary evidence for better accuracy. This is because a positive result on the electronic database will only mean that there is an individual whose personal details correspond to those provided by the client, but not that the client is that individual, its simply an extra piece we use in process but not something we can take at face value.

6.4. Enhanced Due Diligence

The reason why players open player accounts is obvious, so scrutinizing this is not part of the process. However, there may be an ulterior motive like money laundering or funding of terrorism or weapons or drugs, etc. If Plexian Network B.V. has any suspicion that any such activity, then it will conduct further investigations and request for additional data and documentations to either justify its suspicions or else to confirm that there are no justifiable indications of an illegal motive. Sometimes some names are linked to mafia or cartels and that is why in some rare cases additional checks are done to ensure the criminal elements does not use or take advantage of our systems.

There is no specific timeframe or period when these additional checks will be conducted, as these will be simply carried out when the suspicion arises or is determined.

Plexian Network shall implement EDD measures for customers identified as higher risk, with actions tailored to the specific risks identified during the assessment process. These measures aim to intensify monitoring of the business relationship to detect any unusual or suspicious transactions or activities. EDD is required in situations where the risk of ML, TF or PF is heightened.

In any case, the following scenarios are subject to EDD:

- *Residents of High-Risk Geographic Areas*: Customers residing in jurisdictions associated with higher levels of corruption or inadequate AML/CTF regulations.
- *Politically Exposed Persons (PEPs)*: Individuals who hold prominent public positions or are closely connected to such individuals, which may elevate the risk of corruption.
- *Anonymity-Favoring Products or Transactions*: Services or products that allow for a higher degree of anonymity, potentially facilitating illicit activities.
- *New Products and Business Practices*: The introduction of new services, technologies, or delivery mechanisms that may present unforeseen risks.

When the checks are carried out prior to the mandatory period, Plexian Network B.V. will first collect sufficient documentation, and where it is necessary, documentation to establish the player's source of wealth. Identifying the player's source of wealth consists of determining the activities which generate the player's net worth and money they are using to gamble, which will then lead Plexian Network B.V. to determine whether this amount of wealth justifies his projected and actual level of account activity. Plexian Network B.V. will at this stage also profile the player within the player risk profile.

Where the risk determined by following the checks is medium or low, Plexian Network B.V. will accept a declaration from the player with details, such as nature of employment/business, and a declaration regarding annual salary. Searches on professional networks and social media will also be used for verification purposes, like using LinkedIn for example. If the risk is high or Plexian Network B.V. has doubts as to the legitimacy of the items collected, then the player will be requested to provide further independent and reliable documentation which evidences the alleged source of wealth. The goal here is to assure we get their reply on how they earn, so for example: physical proof (like a pay slip) and finally followed by the bank statements showing these earnings being deposited.

6.5. Timeline for Compliance and Non-Compliant Documents

If the customer cannot provide compliant documents within 30 days from the moment the NAf. 4,000.00 threshold is reached, the Company shall terminate the relationship with the customer and consider filing an Unusual Activity Report with the FIU.

During the CDD process, customers may continue to access their accounts while the Company gathers the necessary information. However, if a deposit reaches the NAf. 4,000 thresholds, the customer will be prohibited from further deposits or

withdrawals, although they may continue to play with their existing balance. Conversely, if the threshold is reached due to a withdrawal request, the account will be completely frozen, halting all gameplay.

If a document submitted by a (potential) customer does not meet the verification standards, the compliance officer or designated staff member must immediately flag it for further examination. The initial review should be thorough to pinpoint the specific reasons for non-compliance. Once a non-compliant document is identified, the customer must be informed without delay.

All actions taken in response to non-compliant documents shall be carefully recorded. This includes the initial identification of the issue, communications with the customer, any escalations, and the final outcome. Comprehensive records should be maintained in the customer's file to ensure a complete audit trail.

6.6. Ongoing player monitoring

As described above, the player's account will be successfully opened once the player registers providing the requested basic personal information, and subsequently verifying his email address via the verification code that was sent to his e-mail and must be clicked by the player in order for the account to be born/created. The system is set to prevent minors from registering by rejecting any date of birth inserted which would signify that the player is under eighteen years of age (or any other age as per specific legislation).

Any player details' verification (with the exception of PEP confirmations) may occur at any point in time at Plexian Network B.V.'s discretion. Once the player accomplishes 2k euro in deposits, they are forced to complete the verification process with our team. It makes no difference whether such deposits have been carried out via a single transaction or several transactions, the system will auto force the player to complete this step. Plexian Network B.V. has a system in place which calculates on a daily basis whether the player has reached the deposit limit of 2k euro on their account. An important feature that our system offers is, the identification and prevention of possible multiple accounts, which accounts would have been specifically created to either defraud the company through bonuses abuse or specifically to never reach the required deposit limit of 2k euro and remain undetected, and hence ensuring that the account remains unverified.

Up until the time that this threshold is reached, Plexian Network B.V. will conduct ongoing monitoring to ensure that player information is still correct. Furthermore, if Plexian Network B.V. notices at any point in time any inconsistencies between the information provided by the player and any other information it acquires, Plexian Network B.V. will question the discrepancies and take any remedial action it deems necessary to stop any such fraud or questionable actions. In addition, should it suspect money laundering or funding of terrorism, it will follow the procedure laid out in section 4 below.

Once the mentioned threshold is reached, the player's risk profile will be confirmed, upon the basis of the risk assessment carried out as per our protocols. The latter

shall take place prior to the lapse of thirty days from when the 2k euro threshold is reached. The risk assessment will determine whether the risk posed by the individual is low, medium, or high. The measures adopted to control the risk in question will/can vary, as per the table laid out hereunder:

Risk Identified	Measures Adopted
Low	- Verification of Personal Details (Passport and Utility bill) - On-Going Monitoring is carried out to ensure relationship remains Low Risk and threshold is not exceeded again - Any suspected cases of money laundering or funding of terrorism are to be reported
Medium	- Additional personal details as deemed necessary by Plexian Network B.V. are collected - Verification of Personal Details takes place by using documents containing photographs of the individual - Source of Wealth information is collected - Ongoing monitoring is carried out so as to be able to detect unusual activities, and also to keep information and profile updated - Any suspected cases of money laundering or funding of terrorism are to be reported
High	- Additional personal details as deemed necessary by Plexian Network B.V. are collected - Verification of Personal Details takes place by using documents containing photographs of the individual - Source of Wealth information and documentation is collected - Ongoing monitoring is carried out even more thoroughly and at more frequent intervals than that carried out for medium risk, so as to be able to detect unusual activities, and also to keep information and profile updated - Source of Funds may need to be determined for specific transactions

6.7. Ongoing transaction monitoring

This means the monitoring of clients' transactions is ongoing and always being checked, personal details and any changes in their patterns or wagering preferences (like bet amount or frequency), so as to ensure that they are consistent with the anticipated activity, and if not, to identify why the changes have occurred and try to get a better understanding of those changes. The aim is that subjectively unusual large transactions, changes in gaming patterns and other 'out-of-the-ordinary' activities will be identified and analyzed. In this respect, it is important for Plexian Network B.V. to ensure that the players' information is maintained and kept current/up to date. It will encourage and even force players via the terms and conditions to inform Plexian Network B.V. of any changes, and possibly provide documentation to confirm any justification issued by the player to our team. Through the monitoring process, the risk level will be reviewed and an analysis of whether the previously established risk rating should be amended or not will be carried out. Any inconsistencies in information would need to be justified and Plexian Network B.V. reserves the right to request for further corroborating evidence. Failure to issue information or documentation from new request can result in account closure.

Adequate ongoing monitoring also entails carefully examining the player's transactions and playing patterns so as to ensure that these are in line with Plexian Network B.V.'s knowledge of the player, his gaming activity and risk profile all combined. This is currently being conducted by the player service agents, internal risk/fraud/compliance and payments teams.

Whenever Plexian Network B.V. asks for further information, it will always take note of its findings to evidence its compliance. Should any identified inconsistency persist without it being successfully addressed, Plexian Network B.V. will analyze whether any report is to be submitted to the relevant authorities and or departments and take a decision whether it deems it necessary to suspend the player's account, either temporarily or on a permanent basis.

6.8. Termination of business relationship

Plexian Network B.V. will terminate its business relationship with a player if he fails to provide the requested information and/or documentation, which Plexian Network B.V. has repeatedly requested of the player. Plexian Network B.V. will void any winnings and will then transfer deposited funds to the original source from where the funds originated in form of a refund. All approval for such action must be taken by senior team. If Plexian Network B.V. finds it impossible to remit the funds back to the player through the same channels, it will, as a measure of last resort, remit the funds to a single account held with a credit or financial institution in a reputable jurisdiction in the player's name. In no such refund can be done because the player closed their accounts or cards, then the team can mail out a cheque and or wire transfer to any new account setup by the player.

Whenever remitting such funds, Plexian Network B.V. will indicate in the instructions accompanying the funds that these are being remitted due to inability to complete CDD or failure to comply with our CDD procedures and protocols. Plexian Network

B.V. will also consider whether there are grounds for filing a Unusual Transaction Report (UTR), as per the procedure laid out hereunder.

For accounts that have not been accessed for twelve (12) consecutive months, containing real money balance, such account shall be considered inactive and put into dormancy.

Plexian Network B.V. will contact the client via email up to one month prior to his becoming inactive/dormant in order to advise the player. The player may reactivate an inactive Account by logging in. Once an Account becomes inactive, Plexian Network B.V. will charge an administrative fee to Client's Account, if there is a positive balance in the Account. Such administrative fee shall be 10 Euro (€10) per month or the approximate equivalent thereof in the currency of the territory in which client is a resident. In rare cases, after the player's Account has become inactive and the player accesses the Account once again, Plexian Network B.V. may consider reimbursement of the fees charged if the player can reasonably prove that he could not access the player account due to health-related issues.

6.9. Ultimate Beneficial Owner (UBO) Identification and Verification

Where Plexian Network B.V. establishes or maintains a business relationship with corporate entities, business affiliates, suppliers, payment service providers, or other legal persons, the Company shall identify and verify the UBO(s) in accordance with applicable AML/CFT/CPF legislation.

A UBO is defined as any natural person who ultimately owns or controls, directly or indirectly, twenty-five percent (25%) or more of the ownership interest or voting rights in a legal entity, or who otherwise exercises ultimate effective control over the entity.

The Company shall obtain and verify, at a minimum, the following information:

- Full legal name of the entity;
- Registered address and principal place of business;
- Legal form and registration number;
- Ownership and control structure;
- Full name, date of birth, nationality, and residential address of each UBO holding $\geq 25\%$;
- Identification and verification documentation for each identified UBO.

Verification of UBOs shall be conducted using reliable and independent sources, which may include:

- Corporate registries and official extracts;
- Shareholder registers;
- Group structure charts;
- Notarized declarations of beneficial ownership; and
- Independent commercial databases.

Where no individual meets the 25% ownership threshold, the Company shall identify and verify the natural person(s) exercising senior managing control.

Enhanced Due Diligence measures shall be applied where UBOs are identified as high-risk, including PEPs, sanctioned persons, or individuals located in high-risk jurisdictions.

6.10. Business Affiliate and Supplier Diligence

Plexian Network B.V. may decide to rely on the information but may also get 3rd parties to validate some of the information to assure or help its accuracy. If Plexian Network B.V. decides to rely on information provided by a third party, it may still request the player to provide additional verification documents. When this occurs, Plexian Network B.V. will still conduct the customer-based risk assessment itself, determine the customer's risk rating and conduct on-going monitoring as stated in our protocols above. The relationship between Plexian Network B.V. and the third party will be laid out in an agreement, and one of the conditions will be that of the third party providing Plexian Network B.V. with documents concerning players, immediately upon request. Plexian Network B.V. will also include a Right to Audit clause in the agreement and will indeed periodically test this arrangement, to ensure that the necessary player personal details and documentation is being collected as per the agreed specifications.

Plexian Network recognizes that when contracting or outsourcing specific functions, there is a risk of increased AML exposure if the third parties involved are not properly vetted and their relevant processes are not assessed. Prior to entering into any service agreements that fall under this Policy, Plexian Network performs due diligence to verify the legitimacy of the potential partners. This due diligence includes, at a minimum, obtaining the following documents:

- Certificate of Incorporation
- Identification of Directors and/or Shareholders
- Declaration of Beneficial Ownership
- KYC documentation for signatories, as applicable.

Additionally, where applicable, potential third-party suppliers are required to submit a copy of their AML, CTF and CPF policies and procedures. The CO will review these documents for their accuracy and completeness prior to entering into any agreements.

7. Reporting of unusual transactions and activities

7.1. Appointment of the Compliance Officer (CO)

While the detailed description of the responsibilities of the CO is laid out in the Human Resources Roles and Responsibilities Policy, the CO's main responsibilities will be:

- 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.

The CO will have access to all the necessary information/documentation and company player service agents to effectively carry out his obligations. The CO will act as a contact point between Plexian Network B.V. and the relevant authorities in matters related to anti-money laundering/countering of funding of terrorism.

7.2. What is unusual activity?

The following transactions or intended transactions are deemed unusual:

- a. A transaction, which is reported to the police or judicial authorities in connection with money laundering or the financing of terrorism;
- b. An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c. A transaction amounting to NAf. 5,000.00 or more, regardless of whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner. This includes but is not limited to:
 - A cashless transaction in the amount of NAf. 5,000.00 or more.
 - Accepting or releasing a deposit in the amount of NAf. 5,000.00 or more at the request of the customer;
 - Sale to a customer of chips in the amount of NAf. 5,000.00 or more. "Chips" include but is not limited to tokens and credits.
 - A cash out in the amount of NAf. 5,000.00 or more;
- d. Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Please note that indicators (a) to (c) are referred to as "objective indicators", while (d) is referred to as "subjective indicator". While the objective indicators are based on measurable facts and do not require interpretation automatically classifying a transaction as unusual, the subjective criterion involves a more nuanced assessment, considering the context and behavior of the client. For the purposes of reporting unusual transactions under the objective indicators above, it is noted that the threshold of NAf. 5,000.00 resets per game day of the user.

Plexian Network B.V. shall be obliged to submit a UTR with the FIU with regards to activity carried out.

Plexian Network B.V. staff must be vigilant during the course of their day-to-day activities to gain knowledge of the customers, remain alert of the possibilities of ML and TF and consider whether any customer's activity is unusual and potentially suspicious.

7.3. How to Report unusual transactions and activities

Plexian Network B.V. may have reasonable grounds to suspect that activity on a player account is linked to money laundering or funding of terrorism or drugs, etc. At that point in time, Plexian Network B.V. will ensure that all CDD requirements are met, regardless of whether any applicable threshold has been met or not. It will consequently submit a UTR as soon as possible.

CDD measures which would be adopted in such instances include (but are not limited to):

- Analysis of the customer's account, ID verification and betting history.
- Internal discussions on the case with the Compliance Team and/or the CO;

Making routine follow up queries with the players in accordance with standard practice regarding the background of a transaction or activity. This would NOT be construed as 'tipping off' the player since the reasonable suspicion would still need to be confirmed at this stage.

7.3.1. Internal Reporting Procedures

As laid out in further detail below, all staff communicating with the players, or having access to information about clients' affairs, will receive regular anti-money laundering training. In this manner, staff would be able to identify which player's action should reasonably lead them suspect that money laundering or funding of terrorism activity is being attempted or has been carried out, so they report the event. For instance, if they would be expected to report if a player attempts to register more than one account with Plexian Network B.V., or if he deposits considerable amounts during a single session by means of multiple prepaid cards, then such actions should constitute indicators or red flags which should lead them to question the player's behavior or actions.

At that point, the player service agent may subtly seek explanations from the player, without disclosing his suspicion to the player. This disclosure is forbidden whether directly or indirectly, and why all members of staff must be disciplined in this respect and how they handle the case. If the player service agent does not manage to obtain any convincing information, and after full consideration the agent is still suspicious of foul play, then at that point they shall advise with his supervisor on duty and immediately inform the CO.

Obviously enough, prior to reporting to the CO and completing the internal UTR template (*refer to Appendix 1*) the agent will have to be satisfied that there is a clear indication of intent to circumvent the safeguards, and that use of the financial system for criminal purposes is present.

There may be instances wherein the supervisor disagrees with the officer, but the

player service agent still feels he has reasonable grounds to suspect wrongdoing. In such circumstances, the player service agent is to inform the CO anyway of his suspicions.

The agent may discuss the matter directly with the CO and is in no way obliged to inform or involve his supervisor. On receipt of the internal report from the player service agent, the CO will acknowledge its receipt in writing, referring to the report by its date and unique file number, without including the name of the person(s) suspected.

In this case, the agent's legal obligation to report will be considered to have been fulfilled. The player service agent will only be allowed to discuss the matter internally with management, or with other player service agents, if at all deemed necessary, after having obtained approval from the CO. Any external discussions are prohibited and will be considered tipping off.

If circumstances arise that make it difficult for the player service agent to communicate with the player without risking any possibility of tipping off, the player service agent is to seek advice and follow the CO's instructions on how to proceed. It is of utmost importance that NO internal/external note is made within the customer's account regarding the UTR raised. This procedure shall constitute Plexian Network B.V.'s internal procedure for reporting unusual activity and transactions.

'Tipping off' is an offence under AML/CFT legislation. Officers must be prudent when communicating with the customer, especially if a Unusual Transaction Report (UTR) has been filed with the FIU by the CO, as this may jeopardize the investigation. The CO is to be consulted to guide the player service agent on how to deal with ongoing communications with the player if the circumstances arise. When a customer's account is closed for reasons related to AML/CFT, communication must also be kept general to avoid 'tipping off' the customer.

7.3.2. External Reporting Procedures

As already described in the previous section, the CO shall receive and evaluate internal suspicion reports. He will open and maintain a log detailing the progress related to each report, noting down any information which needs to be documented so as to ensure that an adequate track record of the reasons leading to his decision are maintained. For both internal and external reporting, these records will contain:

- The date of when the disclosure was made;
- The person who made the internal disclosure;
- File Reference number;
- Outcome of the CO review and evaluation.

Such documentation may also be used to assist the Authorities in any analysis or investigation of the suspected money laundering or funding of terrorism when such details are directly requested from the CO. This log shall be held by the CO and shall only be accessible to them and will not form part of the player's file. The CO shall gather all the necessary information and pose any questions to any of Plexian Network B.V.'s player service agent s' as part of his investigation.

The player service agent s (whether those having submitted the internal report or otherwise) shall provide the CO with relevant information. In doing so, they will not be breaching their obligation of client confidentiality. Once the CO decides that there are reasonable grounds which warrant the submission of a UTR via the Authority's submission system, he shall make this formal disclosure to the FIU on behalf of Plexian Network B.V. No copies of either the internal or external reports will be made.

The CO will keep such records secure. The CO shall, where appropriate, inform the originator of the internal report whether or not a formal disclosure has been made. Following a formal disclosure, the CO shall take such actions as required by the Authorities in connection with the disclosure and accordingly follow their instructions.

7.3.3. Reporting Timelines

Employees are required to report any unusual activity to the Compliance Officer immediately, but no later than 24 hours after the transaction has been executed, using the Internal Unusual Activity Report form. If a more in-depth investigation is necessary, the Compliance Officer will complete this within ten (10) business days. During this time, the Compliance Officer may request additional information from relevant departments.

If the Compliance Officer concludes that the activity is unusual, a report shall be submitted to the FIU Curaçao regarding any unusual monetary operations or transactions within 48 hours. In any cases whereby the report is made under one of the objective indicators, as defined below, the report must be made to the FIU Curaçao no later than 48 hours after the transaction has been executed.

7.3.4. Stopping/continuing work following a suspicion

Due to the nature of the gaming products and services offered by Plexian Network B.V., and the nature of the transactions in question, Plexian Network B.V. will not always be in a position to refrain from carrying out a pending transaction prior to the filing of a STR. This is because should Plexian Network B.V. refrain from accepting a transaction when it usually does so instantly, the delay in acceptance may trigger the player into knowing that he is being suspected of fraudulent activity, and therefor tipping them off. Any delay may prejudice an analysis or investigation of the suspected transaction. Hence, whenever Plexian Network B.V. suspects money laundering/funding of terrorism, then Plexian Network B.V. will still proceed with executing the suspected transaction. However, Plexian Network B.V. will, submit an UTR to the FIU immediately after the execution of the transaction.

7.3.5. Disclosure

Plexian Network B.V. will not disclose any details or information in connection with a UTR or a request for information made by the FIU. This prohibition of disclosure applies with regards to both the suspected player and any other third party, and this independently of any other regulatory or contractual obligation that Plexian Network

B.V. may be subjected to. Plexian Network B.V. will also be extremely careful when dealing with a player that is the subject of a UTR or FIU enquiry. As explained above, this is so as not to prejudice an analysis or investigation.

Plexian Network B.V. will also consider carefully any of the measures which it decides to adopt vis-a-vis the suspected player, consequent to the submission of a STR. So as not to jeopardise any investigation, prior to undertaking any such action, Plexian Network B.V. will seek guidance from the FIU's analysts. Plexian Network B.V. will, as much as possible, consider such actions as a measure of last resort, and not unnecessarily burden the FIU with every small suspicion. In cases of minor suspicions not warranting reporting, it will instead increase on-going monitoring and only submit STRs to the FIU once a suspicion persists or the indicators increase. Plexian Network B.V. will ensure proper documentation of such internal decision making.

7.4. Curacao Financial Intelligence Unit

In Curacao, the FIU functions as an administrative buffer between the reporting entities on the one hand and the Public Prosecutor's Office on the other. This buffer, in sorts, prevents transactional information submitted by the reporting institutions from being forwarded to the investigation services: only if there is a reasonable presumption of money laundering and/or financing of terrorism, will the data be furnished to the office of the Public Prosecutor. The Government of Curaçao has opted for the reporting of unusual transactions. If FIU Curaçao, after proper analysis of an unusual transaction, concludes that there is a suspicion of money laundering and/or terrorism financing, this transaction will be reported to the Public Prosecutor's Office as a suspicious transaction.

The company is adamant to report any unusual transactions detected through the FIU goAML portal. This is done in order to maintain the integrity of the financial system and to contribute to the combating of money laundering and financing of terrorism.

8. Payout Management Procedure

Whenever a player makes a withdrawal request, regardless of the payment method used, Plexian Network B.V. will, prior to acceding to such a request, ensure that the institution to which the funds are to be remitted is situated in a reputable jurisdiction. Obviously enough this also ties in to the institutions from where player deposits are accepted. Our policy is, withdrawals will only be processed to the same source from where the funds originated, which is the card or source they used to deposit from. This measure will limit the risk of successful money laundering or funding of terrorism withdrawals.

Withdrawal requests shall be carried out as per the following procedure:

Withdrawal requests will be processed immediately upon request.

The gameplay will be checked as well as all financial transactions.

Plexian Network B.V. will also consider whether individuals are playing fairly, or whether the gaming system has in any way been manipulated, or whether the system is, alternatively, malfunctioning, and the player was in any way taking advantage of any bug without, accordingly informing Plexian Network B.V., as per the Terms and Conditions' requirements and agreed by the player before creating

and using our paid services.

Reference will also be made as to whether CDD verification has been conducted. If it has not yet been carried out since the deposit requirement was not reached, a management decision is taken as to whether it is deemed necessary to conduct CDD verification at this stage prior to completing the withdrawal process.

The risk assessment is also conducted / checked to ensure that the player's risk vis-a- vis his activity with Plexian Network B.V. is determined.

Applicable CDD requirements will be as per section 3.2 above.

If the player does not provide the necessary documents for verification to take place, when requested, or if it becomes clear that verification cannot take place because the individual has acted fraudulently, withdrawals will not be processed. Once it becomes clear to Plexian Network B.V. that the individual was attempting to act fraudulently, it will block the player's account, void all winnings and simply return the deposit to the account from where the funds originated.

In the event that withdrawals cannot be processed to the account from where the funds originated, then Plexian Network B.V. will formally request for player verification documents and also request for details of another payment system that may be confirmed to be in the player's name and hence minimizing the risk of remitting funds to an individual that is different from the person that had originally remitted the deposits. This process is in place to discourage credit card theft and identity theft.

9. Employee Screening and Training

Employee due diligence is a process employed to screen employees with the objective of identifying and reducing Plexian Network's exposure to the risks associated with money laundering and terrorism financing. These procedures apply not only to the Company's contractual employees, but also to its contractors and subcontractors.

The employee due diligence process is informed by Plexian Network's risk assessment and the specific roles within the organization.

Any employee whose position may enable them to facilitate money laundering or terrorism financing must undergo screening. This requirement applies to prospective employees prior to their hiring for such roles, as well as current employees before they are transferred or promoted to such positions. Regular updates and re-evaluations are essential for maintaining an effective compliance program against ML, TF and PF. This process includes conducting periodic reviews of all employees, with a particular emphasis on those in high-risk roles, to ensure their risk profiles are accurate and current.

To screen both current and potential employees, Plexian Network will:

- Identify the individuals;
- Verify their identity;
- Confirm their employment history, such as through references; and
- Determine their suitability for the position and assess whether they pose any risk to the Company.

Positions that may render an employee vulnerable to collusion with or coercion by criminal organizations should undergo more rigorous checks. Plexian Network must evaluate whether:

- The employee has a criminal record, which may be verified through a police check.
- The employee is or has been subject to regulatory, court, or legal actions.
- The employee has leveraged bankruptcy laws for personal gain.
- The employee has resided in high-risk countries or regions.

It is the policy of Plexian Network B.V. that all staff who have client contact, or access to information about clients' affairs, shall receive anti-money laundering training to ensure that their knowledge and understanding is at an appropriate level. Training will furthermore be provided at least once a year so as to maintain awareness and ensure that the company's legal obligations are met. Any training given will take into consideration the practicality of assigning different tasks to staff as per their role, and all information accessible will be on a need-to-know basis. However, training about the whole process will be provided to player service agents, so as to ensure that each player service agent has a holistic understanding of the due diligence, KYC, AML and payout procedures, since these are very closely related.

In light of the seriousness of the obligations placed by law and regulations, and the

gravity of the possible penalties, the CO shall ensure that information about these obligations is available to all members of staff at all times. The CO will also ensure that on-going training is provided, that is, as and when the need arises, even based on direct requests made by player service agent s.

The training programs will include testing to ensure that each individual has achieved the appropriate level of knowledge and understanding. Testing may be conducted in various ways, whether through formal testing, assessment via discussion of case studies, or other means. Special consideration will be given to the training needs of senior management, and of the compliance team, whose knowledge and understanding must be most thorough.

The Human Resources (HR) Department will:

- ✓ inform every member of staff of the training programs that they are required to undertake, and the timetable for completion;
- ✓ check that every member of staff has completed the training programs assigned to them, issuing reminders to any who have not completed the programs as per the applicable timetable;
- ✓ keep records of training completed, including the results of tests or other evaluations demonstrating that each individual has achieved an appropriate level of competence;
- ✓ update player service agent personal files with details of training undertaken and results obtained where applicable;
- ✓ refer to senior management any cases where members of staff fail to respond or whose results are unsatisfactory, to issue reprimands or provide additional training as per the individual case.

The CO will be provided with full access to all records held by the HR Department. On completion of a training cycle, the HR Department will ensure the continuity of ongoing training and also obtain updates from the CO in respect of changes happening in the field, so that the HR may ensure that up-to-date training is organised and provided to all members of staff.

Line managers will also provide feedback to the HR Department in respect of:

- ✓ the effectiveness of the programs completed; and
- ✓ make suggestions as to different methods of delivery.

Line managers will supplement the training provided to support staff by giving guidance on a day-to-day basis on:

- ✓ the type of client instructions and transactions that count as 'significant' and so should be brought to their attention
- ✓ identifying client instructions and transactions which, although not of a nature normally counting as 'significant', are in some way unusual or anomalous and should be considered with regard to possible suspicion of money laundering or funding of terrorism.

The CO will determine the training needs for his/her own role, and ensure that he/she undergoes Continued Professional Education (CPE) as required to fulfil his/her legal obligations.

The aim of all training provided is to ensure that staff is capable of identifying any attempted or actual money laundering or funding of terrorism activity exercised by players when using Plexian Network B.V.'s services.

10. Independent Audit Function

Plexian Network B.V. shall maintain an independent audit function to periodically test and evaluate the effectiveness, adequacy, and compliance of its Anti-Money Laundering, Counter-Terrorist Financing, and Counter-Proliferation Financing (AML/CFT/CPF) framework.

The independent audit shall be conducted at least once every two (2) years, or more frequently where required by regulatory developments, material changes to the business model, or the identification of significant compliance weaknesses.

The audit function shall be independent from the operational AML processes and may be performed by:

- An internal audit function independent from AML operations; or
- An external, suitably qualified and independent third party.

The scope of the audit shall include, at a minimum:

- Assessment of the effectiveness of the AML/CFT/CPF policies, procedures, and internal controls;
- Testing of customer due diligence (CDD), enhanced due diligence (EDD), and ongoing monitoring measures;
- Review of unusual transaction reporting processes and regulatory filings;
- Evaluation of record-keeping practices;
- Review of employee training and awareness programs; and
- Assessment of compliance with applicable Curaçao AML/CFT/CPF laws and CGA regulations.

The findings of the independent audit shall be documented in a written report and submitted to senior management and the Board of Directors. Any identified deficiencies shall be addressed promptly through a documented remediation plan, with follow-up actions monitored by the Compliance Officer.

11. Keeping records of client due diligence information

When information is being collected for CDD purposes, the responsible service staff will:

- ✓ keep records in the client file.
- ✓ record instances where information requested has not been forthcoming, or explanations provided have not been satisfactory.
- ✓ ensure that all records are kept in a consistent manner so that they are accessible by and comprehensible to other authorised members of staff, including the CO.

Plexian Network B.V. shall maintain comprehensive records of all customer due diligence, transaction monitoring, and reporting activities in accordance with applicable AML/CFT/CPF legislation.

Records to be retained include, but are not limited to:

- Customer identification and verification documents (CDD and EDD);
- Beneficial ownership information;
- Risk assessments and risk classifications;
- Transaction records, including deposits, withdrawals, and payment methods;
- Unusual Transaction Reports (UTRs) and related internal documentation;
- Correspondence with customers relating to AML matters;
- Training records and audit reports.

All records shall be retained for a minimum period of five (5) years from:

- The date the business relationship ends; or
- The date of completion of an occasional transaction,

whichever occurs later.

Records shall be stored securely, in a manner that ensures confidentiality, integrity, and availability, and must be capable of being made available without undue delay to the Curaçao Gaming Authority, the Financial Intelligence Unit (FIU), or other competent authorities upon lawful request.

11.1. Internal Procedure for Submitting a UTR

- All emails regarding players activities and/or transactions must be sent to support@usoftgaming.com to the attention of the Compliance Officer, William Dornat, with subject line always containing "UTR Submissions"
- The email should include the UTR completed with the relevant details (*Refer to template in Appendix 1 hereunder*).
- The UTR should include (*but is not limited to*) the following details:
 - The customer's name or system ID and the unusual transaction(s) or activity reported

- If the reason for your suspicion is directly linked to an automated alert generated, include the alert reference
- A brief explanation as to why you find the transaction or activity unusual and why it may relate to money laundering or terrorist activity and explain what has happened with the player e.g. has account been suspended, what action has been taken (if any)
- If the finding relates to a third party, set out the details of the third party and what information you find risk-increasing.
- The CO will acknowledge your email, review the case and advise on any next steps

11.2.Examples of Unusual Transactions

- i. Player deposits money and immediately requests to cash out with no logical explanation;
- ii. Player sent an email to change his name to avoid the tax authorities finding out about his winnings;
- iii. Player created a new account, deposited maximum amount via the payment card and immediately bet on the same horse at the same race two minutes prior to the race commencing;
- iv. Significant or unusual pattern of deposits, minimal or no play (with no explanation such as self-exclusion of vacation), followed by a withdrawal (possibly to another payment method);
- v. Suspicious player identification details believed to be false or altered;
- vi. Repeated incorrect verification of player details;
- vii. Attempts by the player to bribe, corrupt or unduly influence to change transaction data or sensitive ID data;
- viii. Abnormal re-routing of funds;
- ix. Attempts to create a false account with an unusual deposit;
- x. Players creating a new account and depositing in a short space of time (a quick deposit);
- xi. Players funding their account for the first time by using the maximum deposit allowed;
- xii. Various card being used/attempted to be used to fund an account in a short period of time;
- xiii. The profile of the player (age, location, maybe time of day do not seem realistic);
- xiv. Players funding their accounts with various smaller amounts deposits over a short period of time;
- xv. New player moving quickly between products;
- xvi. New players playing through deposits very quickly and immediately withdrawing any winnings;
- xvii. Safeguarding (Players continually staking equal amounts on red and black on roulette);

12. Appendix 1: Unusual Transaction User Report Template

Report Date	
--------------------	--

Part 1: Sign Up Details

User Account Number:	
Alias:	
First name:	
Last name:	
Address:	
Country:	
Email:	
Computer ID:	
Date of birth:	
Phone:	
Mobile:	

Sign up date:	
Last login date:	
Sign up Ip address:	
Sign up Ip ISP:	
Sign up Ip city:	
Sign up Ip country:	

Google Maps address link:	
----------------------------------	--

Part 2: Unusual Activity Information

Date or date range of unusual activity				
Type of unusual activity	☐	Minimal gaming with large transactions		
	☐	Unusual use of wire transfers		
	☐	Terrorist financing		
	☐	Money Laundering		
	☐	False or conflicting identification documents		
	☐	Credit/debit card fraud		
	☐	E-Wallet fraud		
Details of unusual activity				
User acted alone or part of a group	☐	YES	☐	NO
If YES enter the Account ID				
How did investigation started.	☐	Internal monitoring		
	☐	Reported by the bank		
	☐	Reported by E-Wallet provider		
	☐	Reported by the police		
3rd Parties informed	☐	None		
	☐	Issuing card bank		
	☐	E-Wallet provider		
	☐	Police		

Part 3: Payment Details

Account Currency:	☐	USD	☒	GBP	☐	EUR
-------------------	--------------------------	-----	-------------------------------------	-----	--------------------------	-----

****Payment method/s used to be updated accordingly****

Type of payment option used for deposit:	
Type of payment option used for Withdrawal:	

Last 4 digits of Card:		
Card End Date:		
Name on Card:		
Card Issuer:		
Card Issuing Country:		
Credit Card Type:		

Part 4: Deposit and Withdrawal Information

Total Deposit:	
Total Withdrawals:	

Deposit Date and Time:	Deposit Amount:

Withdrawal Date and Time:	Withdrawal Amount:

Deposit IP Address:		
Deposit IP City:		
Deposit IP ISP:		
Deposit IP Country:		

Withdrawal IP Address:		
Withdrawal IP City:		
Withdrawal IP ISP:		
Withdrawal IP Country:		

Part 5: Account Verification

Documents Requested:	☐	YES	☐	NO
If YES enter date				
Documents Received:	☐	YES	☐	NO
Phone Verified:	☐	YES	☐	NO
Email Communication:	☐	YES	☐	NO
Social Network Verification:	☐	YES	☐	NO
If YES enter link				

Copy any documents or communication that we receive from user.

13. Appendix 2: Country Risk List

PLexian Network B.V. - AML/CFT

Please note that the following list of high-risk and low-risk countries is subject to continuous review. Any changes in geographical risk will be reflected promptly to ensure the list remains current and accurate.

High-risk countries include:

1. Afghanistan
2. Algeria
3. Angola
4. Belarus
5. Bulgaria
6. Burkina Faso
7. Burma (Myanmar)
8. Cameroon
9. Central African Republic
10. China
11. Côte d'Ivoire
12. Croatia
13. Cuba
14. Democratic People's Republic of Korea
15. Democratic Republic of the Congo
16. Ethiopia
17. Gibraltar
18. Haiti
19. Iran
20. Iraq
21. Kenya
22. Lebanon
23. Libya
24. Mali
25. Monaco
26. Mozambique
27. Namibia
28. Nicaragua
29. Nigeria
30. Panama
31. Philippines
32. Russia
33. Somalia
34. South Africa
35. South Sudan
36. Syria
37. Tanzania
38. Uganda
39. United Arab Emirates
40. Vanuatu
41. Venezuela
42. Vietnam
43. Yemen

7. Dominica
8. Finland
9. Grenada
10. Guyana
11. Montserrat
12. New Zealand
13. Norway
14. Saint Kitts and Nevis
15. Saint Lucia
16. Saint Vincent & the Grenadines
17. Singapore
18. Sint Maarten, Kingdom of the Netherlands
19. Suriname
20. Sweden
21. Turks and Caicos Islands

Excluded markets include, but are not limited to:

1. Aruba
2. Australia
3. Austria
4. Belgium
5. Bonaire
6. Czech Republic
7. Curaçao
8. France
9. Germany
10. Greece
11. Lithuania
12. Saba
13. Sint Eustatius
14. Spain
15. The Netherlands
16. United States of America

Low-risk countries include:

1. Antigua and Barbuda
2. Aruba, Kingdom of the Netherlands
3. Belize
4. Bermuda
5. Canada
5. Cayman Islands
6. Denmark