

Play UK Internet N.V.

Hoogstraat 18-22, unit 3.6

Willemstad, Curaçao

AML/CFT MANUAL

May 2025

Table of Contents

Contents

REVISION HISTORY	4
DEFINITIONS AND ABBREVIATIONS	5
1. AML/CFT Policy	7
1.1 Policy	7
1.2 Objective	8
1.3 Scope	9
2. Regulatory Framework	9
2.1 National regulations	9
2.2 International regulations	10
3. Procedures	11
3.1 Risk Management	11
3.1.1 Risk assessment	11
3.1.2 Risk Classification	14
3.2 Customer Due Diligence	15
3.2.1 Know Your Customer (KYC)	15
3.2.2 Due Diligence	16
3.2.3 Politically Exposed Persons	18
3.2.4 Beneficial Ownership Identification & Verification	19
3.2.5 The Risk Department	19
3.3 The Monitoring of Account Holder activities	20
• Multiple accounts	21
• Identity fraud	21
• Unusual activities	21
• Withdrawal, deposit or pay out of funds	22
• Prior review of account activity	22
3.4 Transactions using Cryptocurrency	23
4. Money Laundering Reporting Officer (MLRO)	24
4.1 Ongoing monitoring	24
4.2 Reporting of unusual transactions	25
4.3 Record keeping	25
4.4 Training	26
4.5 Staff Due Diligence & Whistleblower Protection	26
4.6 Periodical review of AML/CFT policies	26
5. Ongoing monitoring policy	27
5.1 AI-driven transaction monitoring with:	27
5.2 Dynamic risk reassessment:	27
5.3 Biometric verification checks:	27
6. Timing of Customer Due Diligence (2025 Regulations)	27

6.1	Initial CDD	27
6.2	Ongoing CDD	27
6.3	Event-Triggered CDD	28
7.	Reporting Obligations under Curaçao's 2025 AML Regulations	28
7.1	Suspicious Activity Reports (SARs)	28
7.2	Threshold Transaction Reports	29
7.3	Beneficial Ownership Updates.....	29
7.4	Monthly Aggregate Reporting	29
8.	Termination of Business Relationship Policy (2025 Curaçao AML Regulations).....	29
8.1	Mandatory Termination Triggers.....	29
8.2	Termination Protocol	30
8.3	Prohibited Activities	30
8.4	Exceptions Process.....	30
9.	Reliance on Third Parties for AML Compliance.....	30
10.	IT Security Measures for AML Compliance.....	31
Annex A		32

REVISION HISTORY

Version #	Date Issued	Author	Reviewer	Approved By
1.0	March 30, 2021	EM Group	Operations	Mr. G. van Zinnicq Bergmann - MD
1.2	January 2024	Operations	Legal Department	Mr. G. van Zinnicq Bergmann - MD
2.0	October 8, 2024	EM group	Operations	Mrs. A. Heyer – MD
3.0	May 23, 2025	Moneeb Jaffari	Compliance Officer	Pending

DEFINITIONS AND ABBREVIATIONS

Account Holder:	an individual who applied and was granted an account held at the internet gateway operated by the Company for the use of the provided Services.
AML:	Anti Money Laundering. All efforts focused on the prevention of transforming proceeds obtained from criminal activities into funds which appear to be obtained from legal activities.
CFT:	Combating the Finance of Terrorism. All efforts focused on the prevention of providing funds at the disposal of terrorists to be used for committing terrorist attacks.
CPWMD:	Efforts focused on combatting the sale, transfer and export of nuclear, chemical or biological weapons and their means of delivery and related materials.
The Company	Play UK Internet N.V., a limited liability company under the laws of Curaçao, registered with the Chamber of Commerce of Curaçao under number 95091.
FATF:	Financial Action Task Force (www.fatf-gafi.org)
FIU:	the Financial Intelligence Unit of Curaçao.
KYC:	Know Your Client, the mandatory process of identifying and verifying the client's identity when opening a Player Account and periodically over time.
MLRO:	Money Laundering Reporting Officer
Non-reputable Jurisdiction:	Country mentioned on the list of the FATF as jurisdictions for which a call of action has been issued or are mentioned on the list of monitored jurisdictions.
Player:	Individual who has registered with the Company for the purpose of making use of the Services offered on the Website and for which an account has been opened providing him/her with a unique code.
Player Account:	an account granted to an individual after registration. The account is created and issued by the Company and is required for wagering with real money. Only one Player Account is permitted per person, per family and per Shared Environment.
PEP	Politically exposed person.

Shared Environment	an environment that has a common internet connection which includes but is not limited to airplanes, households, universities, libraries, cyber cafes, coffee shops and work forces.
Service:	the gaming and betting offers provided by the internet gateway operated by the Company to the Account Holder, through the Website.
Website:	the websites mentioned under Annex A, which are operated by the Company.

1. AML/CFT Policy

1.1 Policy

Money Laundering, Terrorism Financing and Proliferation of Weapons of Mass Destruction are some of the ever-growing threats for national and international economies throughout the world, forcing all vulnerable sectors to have measures in place for the prevention of their misuse for these purposes. Individuals involved in ML, TF and PWMD continually attempting to exploit services and products to conceal their unlawful activities and proceeds' true nature. Illicit efforts by such individuals must be recognized and thwarted by all feasible means. AML policies incorporate regulations and laws for limiting financial criminals from concealing funds collected through illicit sources.

ML in the online gaming industry manifests itself in two opposing forms:

- a. the use of criminal funds to fund gambling activities; and
- b. the exchange of criminally acquired funds for legitimate money.

In both cases, authorities fear that those phenomena damage sports, the online gaming industry, and society as a whole. Therefore ML, when not eliminated, can have far-reaching implications.

TF may not involve the proceeds of criminal conduct but rather an attempt to conceal the origin or intended use of the funds, which will later be used for unlawful purposes. Terrorists regularly adapt how and where they raise and move funds and other assets in order to circumvent safeguards that jurisdictions have put in place to detect and disrupt this activity. Identifying, assessing and understanding TF risks is an essential part of dismantling and disrupting terrorist networks, as well as the effective implementation of the risk-based approach of CFT measures. PFWMD may involve the sale, transfer, export, of weapons of Mass destruction, like nuclear weapons and atomic weapons. Such proliferation must be countered as well due to it posing a significant threat to international peace and security, as identity by relevant United Nations Security Council Resolutions (UNSCRs). Therefore, the CP measures involve identifying and assessing the risks of potential breaches or evasion of the targeted financial sanctions to proliferation financing and taking appropriate mitigating measures with the level of risks identified.

Targeted Financial Sanctions (TFS) refer to legally mandated restrictions requiring immediate freezing of assets and prohibition of financial dealings with individuals, entities, or organizations designated by Curaçao's government (under Sanctions National Decree N.G. 2010, no. 93), the United Nations, or other international bodies due to their involvement in terrorism, terrorist financing, or proliferation of weapons of mass destruction. These sanctions, which form a critical component of Curaçao's AML/CFT framework alongside the National Ordinance on Money Laundering (P.B. 1993, no. 52) and other regulations, obligate financial institutions to

continuously screen clients and transactions against updated sanctions lists, promptly freeze any identified assets, and report matches to the Financial Intelligence Unit, with no prior transactions permitted unless authorized by competent authorities.

The Company takes AML/CFT/CPF seriously and has policies in place to ensure compliance with the regulations in the jurisdictions where we operate. The Company's procedures and internal controls are designed to ensure compliance with all applicable national and international regulations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in applicable law and changes in our business.

1.2 Objective

The Company is a limited liability company, duly incorporated and registered in accordance with the laws of Curaçao. This policy is written based on the national legislation on AML, CFT, CPWMD and the penalization of predicate crimes of Curaçao and applicable international standards set by the FATF. Combined, these regulations provide a solid, internationally accepted standard for the procedures maintained for the prevention of the misuse of the Services provided by the Company.

This Policy outlines the AML/CFT strategy of the Company in order to:

- a. ensure that statutory and regulatory obligations to prevent ML and FT are met, taking positive action to minimize risk of the Company's products and services being used for the purpose of laundering funds and using proceeds of criminal activity, or terrorist financing.
- b. ensure that the Company does not engage with or continue established relationships with those whose conduct gives rise to suspicion of involvement with ML and/or TF;
- c. terminate any relationships where the Account Holder's conduct gives the Company reasonable cause to believe or suspect involvement with illegal activities. Any such termination shall follow the reporting of the suspicion and thereafter shall be undertaken in conjunction with the relevant authorities and in accordance with the relevant regulations; and
- d. comply with the Company's AML and, CFT and CPF obligations based on national and international regulations.

Proper Identification of Account Holders, verification of the identity, monitoring of Player activities and reporting of unusual activities are part of the measures the Company has in place in an effort to prevent, deter or mitigate industry related risks.

1.3 Scope

The Company is committed to the highest national and international AML and CFT standards when providing its Services and is applicable to Employees, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external contractors, third-party representatives and business partners, sponsors, or any other person associated with the Company that falls within the scope of the Company's AML Policies.

This Policy defines procedures that will assist all persons working for the Company to comply with its legal obligations. Failure of an Employee to comply with the procedures defined within this Policy may lead to disciplinary action.

2. Regulatory Framework

2.1 National regulations

Pursuant to the Code of Criminal Law (Penal Code) (N.G. 2011, no. 48), money laundering is a criminal offence in Curaçao. Further main national regulations relating to money laundering and terrorist financing are amongst others:

- a) The National Ordinance on Money Laundering (P.B. 1993, no. 52);
- b) The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G. 2024, no. 41 (N.G. 2017, no. 92) (NORUT), together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- c) The National Ordinance on Identification of Clients when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2009, no. 66 (N.G. 2010, no. 40) (NOIS), together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- d) The National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification of Clients when rendering Services (National Decree containing general measures on Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70);
- e) Sanctions National Decree Al-Qaida c.s., the Taliban of Afghanistan c.s., Osama bin Laden c.s., and terrorists to be designated locally (N.G. 2010, no. 93);
- f) National Ordinance on the Obligation to Report Cross-border Money Transportation (N.G. 2002, no. 74), together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;

- g) National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (AML/CFT Ordinance) (Landsverordening ter voorkoming en bestrijding van witwassen en terrorismefinanciering), expected in P.B. 2023/2024, introducing enhanced due diligence, expanded reporting obligations, and regulation of virtual asset service providers (VASPs);
- h) Amendments to the Sanctions Framework, including updates to the Sanctions National Decree (N.G. 2010, no. 93) to incorporate newer UN/EU-listed terrorist entities and proliferation risks.

These laws and decrees serve as the basis for the procedures maintained by the financial sector of Curaçao to detect and deter industry related risks for money laundering, the financing of terrorism or other criminal activities.

2.2 International regulations

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 these standards in its national legislation.

On international level, the FATF plays a very important role in the combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction. The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures and promotes the adoption and implementation of appropriate measures globally.

In performing these activities, the FATF collaborates with other international bodies involved in combating money laundering and the financing of terrorism. In total 34 countries are direct members of the FATF and through regional organizations over 180 countries are connected to the FATF.

Subsequently the present policy is a combination of the FATF and local AML/CFT rules and regulations. This ensures a solid, internationally accepted basis regarding AML/CFT. In case local laws and regulations require additional compliance duties, the Company is free to develop additional procedures to comply with local regulations.

3. Procedures

In an effort to be compliant with the applicable rules, regulations and international standards, the Company has procedures in place to which it attains itself to when providing Services to Account Holders. These procedures cover the following standards:

- Risk Management
- Risk Classification
- Customer Due Diligence
- Know Your Client
- Due Diligence
- The Money Laundering Reporting officer
- Monitoring of Account Holder activities
- Reporting of unusual transactions
- Recordkeeping

3.1 Risk Management

3.1.1 Risk assessment

The possibility of online gaming being used by criminals to assist in ML, PWMD and/or TF poses many risks for the Company, such as criminal and regulatory sanctions and/or reputational damage for the Company and/or its Employees. For this purpose, the Company must carefully identify its risks and manage them accordingly.

The Company takes the following steps to manage its risks appropriately:

- i. identifying the ML, PWMD and TF risks relevant to the Company;
- ii. assessing the level of risk;
- iii. understanding the impact of the risk;
- iv. designing and implementing appropriate policies, procedures and controls to manage and mitigate these risks;
- v. monitoring and improving the effective operation of these controls and identifying any weaknesses; and
- vi. recording what has been done and why.

In view of the above, the Company must conduct a risk assessment to analyze the risks faced by the Company and ensure that the identified risks are properly mitigated and resources adequately invested.

The risk assessment must identify and analyze the risks related to the following four key risk

sources stemming from inherent vulnerabilities in the online gaming sector:

- i. Account Holders
- ii. Product / service / transactions
- iii. Interface
- iv. Geography

The Company must review its risk management processes on an on-going basis to ensure that it remains abreast of new risks. As a minimum, the risk assessment must be reviewed annually, or more frequently in the case of any important changes to products or technology, payment methods, customer type and other material changes.

The risk assessment will also analyze the policies, procedures and systems of the Company in order to ensure that the identified risks are properly mitigated through the adoption of robust policies and procedures. The results of the risk assessment will serve as the foundation to determine the Company's risk appetite. The following risk areas should be considered by the Company for the purpose of the risk assessment:

Account Holder Risk

The risk of ML/FT may vary in accordance with the type of Account Holder. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. An Account Holder having a single source of regular income will pose a lesser risk of ML/FT than an Account Holder who has multiple sources of income or irregular income streams.

Product/Service/Transaction Risk

Some products/services/transactions are inherently riskier than others and are therefore more attractive to criminals. These include products/services/transactions which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the Account Holder to influence the outcome of a game, be it on his own or in collusion with others. The use of specific funding methods should also be treated as high risk factors. This includes cash and other similar or anonymous payment methods that may not leave or disrupt the audit trail and allow the Account Holder to operate with a degree of or complete anonymity such as pre-paid cards or virtual currencies. The exceptional use by an Account Holder of Player Accounts held or cards issued in the name of third parties is also to be regarded as a high-risk factor. Conversely, where an Account Holder transfers funds from a bank account or a card linked to a bank account held in his name with an institution established in a reputable jurisdiction, the risk of ML decreases.

Interface risk

Channels through which a business relationship is established and/or through which transactions are carried out may also have a bearing on the risk profile of a business relationship or a transaction. Channels that favor anonymity increase the risk of ML/FT if no measures are taken to address the same. While situations where interaction with the Account Holder takes place on a non-face to face basis will no longer lead to the relationship being considered as automatically high risk, interacting in this manner is still to be considered as a high risk factor for risk assessment purposes.

Table 1000000

	GAME TYPES				
	Low	Low-Medium	Medium	Medium-High	High
Fixed odds games without hedging (ex: slots, lotteries, bingo)	X				
Fixed odds games where hedging is possible (blackjack, baccarat, roulette)			X		
Sportsbetting			X		
P2P games (ex: poker, betting exchange)					X

	FUNDING METHODS				
	Low	Low-Medium	Medium	Medium-High	High
Bank transfers (EEA or equivalent safeguards)	X				
Debit/credit cards issued by banks (EEA or equivalent safeguards)	X				
Debit/credit cards issued by other licensed financial institutions		X			
EEA-licensed payment service providers			X		
Non-EEA licensed PSP				X	
EEA-licensed PSP that can be funded with cash or quasi-cash				X	
Prepaid cards/vouchers					X
Cash					X

Geographical Risk

The geographical risk is the risk posed to the licensee by the geographical location of the business/economic activity and the source of wealth/funds of the business relationship. The nationality, residence and place of birth of an Account Holder have to be taken into account as these might be indicative of a heightened geographical risk. Countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of

mass destruction as well as countries which are known to have terrorist organizations operating within are to be considered as high risk. The opposite is also true and may therefore be considered as presenting a medium or low risk of ML/FT.

In order to identify and manage potential hazards, the high-risk territories are the next:

- i. Prohibited Jurisdictions: these jurisdictions are prohibited under the Curaçao license conditions and/ or pursuant to a resolution of the Company's managing director;
- ii. jurisdictions which are identified by FATF as high-risk jurisdictions subject to a call for action;
- iii. jurisdictions under increased monitoring by FATF;
- iv. countries which are identified by the European Union as high-risk countries;
- v. countries which are identified by the United States as state sponsors of terrorism.

3.1.2 Risk Classification

Upon registration, the Company makes a risk classification of each Account Holder.

The Company maintains the following risk classification:

- Low risk
- Medium risk
- High risk

The level of due diligence that should be performed on the Account Holder is determined based on the risk classification above.

Type of Account Holder	Monitoring frequency
Account Holders who are under active investigation or suspected in ML/TF or other fraudulent activity and their accounts are not limited for deposit or logins	Daily
PEPs, which are deemed to present a high risk	Daily
High-Risk Account Holders, High-Rollers, PEPs with lower relative risk and active Account Holders from high-risk jurisdictions	Weekly (or upon a material change)

Medium Risk Account Holders	Every six months (or upon a material change)
Low Risk Account Holders	Annually (or upon a material change)

3.2 Customer Due Diligence

3.2.1 Know Your Customer (KYC)

Following international standards and local applicable legislation, it is imperative for a company to know its clients. A sound KYC policy and procedure are critical in protecting the safety and soundness of a company and the financial system. In line herewith the Company has the following procedures in place.

KYC information request

An individual cannot participate in a game for money unless that individual has registered and has been provided with a Player Account. Only one Player Account is permitted per person, per family and per Shared Environment.

To comply with Curaçao's AML/CFT laws (including NOIS N.G. 1996, no. 23) and FATF Recommendation 10, players must provide:

1. Identity Verification:
 - Full legal name (first and last name).
 - Nationality (mandatory for sanctions screening and risk assessment).
 - Date of birth + valid government-issued ID (e.g., passport, driver's license) proving age (18+ or local majority age).
 - ID card number (or passport number for non-residents).
2. Contact Details:
 - Current full residential address (no P.O. boxes).
 - Valid email address and telephone number.
3. Financial Details:
 - Payment method information (e.g., bank account, e-wallet) linked to the player's name.
4. Account Security:
 - Unique username and password.
5. Additional Data (if applicable):
 - Gender (for identity cross-verification).
 - Source of funds/wealth (required for high-risk players under EDD).

The name on the account must match the true, legal name and identity of the individual. The

username, password and other personal information related to the account must be kept secret and confidential and may not be used by any third party. In case of a suspected violation, an Account Holder must request new log-in credentials.

On registration, a geographical location check is carried out on the applicant's computer IP to ensure that person is in a permitted jurisdiction. If the applicant is not in a permitted jurisdiction, he/ she will not be allowed to have a Player Account.

The Company proceeds to review the information provided and may request additional documentation in order to verify the provided information. The Player Account may be put on hold until satisfactory information has been received or terminated if the Company finds the information contained in the Player Account to be false or misleading.

The Company reserves the right to refuse to open or close a Player Account at its own discretion following review of the provided KYC information.

Log in details

It is not permitted for a Player to share the login details to access the system with a 3rd party. The Company reserves the right to cancel, without refund, a Player Account if the login details were disclosed to a 3rd party.

3.2.2 Due Diligence

Standard Due Diligence

All applicants are required to submit proof of identity, proof of address and payment ID at the time of deposit of funds or where applicable at any given time requested by the Company.

The Company requests the following information to verify the identity of the Player:

1. A driver's license or valid passport;
2. Identity card;
3. A recently issued copy of a utility bill not older than three months or bank statement.

Notwithstanding the checks that are performed during the onboarding of a Player, there is also a Standard Due conducted in other instances as stated below. Standard Due Diligence is conducted, amongst others, in the following cases:

- upon a request for withdrawal;
- when a threshold of a single or cumulative transactions of EUR 2,000 or equivalent is reached;
- anytime at the discretion of the Company.

The Company further reserves the right to conduct a phone verification of the Player Account to verify details provided by the Player at the time of registration or at any other time requested by the Company. The details include but are not limited to name, home address, email of the registered Player Account holder, phone number, photo ID, payment methods, bet types, amounts and event details. Failure to satisfactorily complete this verification due to the previously provided details being fake, false, incorrect, misleading, non-existing, not belonging to the Player or unable to be verified, may result in the Company closing the Player Account and the confiscation of any winnings. In case the Company discovers that a transaction in the course of the business relationship of an amount of € 2000,- or more takes place, then the Company must perform verification of the Account holder's identity prior to accepting more transactions of the Account holder taking place.

In addition, the Company screens all applicants against international sanctions lists in order to prevent those sanctioned individuals open a Player Account.

Enhanced Due Diligence

In certain specific instances the Company will conduct Enhanced Due Diligence by requesting the following KYC information:

1. A driver's license or valid passport;
2. A selfie of the Player holding the identification document;
3. A recently issued utility bill or bank statement
4. A bank statement showing the initial deposit;
5. A bank statement no older than 3 months from the bank to which a withdrawn amount should be deposited;
6. Information regarding the source of wealth.

Enhanced Due Diligence is applied as soon as a Player is classified as a High risk including but not limited to the following situations and as further discussed in the section 'Monitoring of Account Holder activities':

- upon suspicion of a Player attempting to or having created multiple Player Accounts in multiple different names;
- upon suspicion of Player(s) being part of a syndicate of Players colluding to gain an advantage over the Company;
- upon suspicion of the Player being a politically exposed person (PEP);
- at the detection of any irregular, suspicious, inappropriate or fraudulent activity;

- anytime, at the discretion of the Company.

If at the discretion of the Company, the provided information is considered unsatisfactory or is suspected to be fraudulent or obtained from a third party to perform illegal operations on the site, the Company will engage third party agencies to confirm the provided information on the identity and the payment details. This process entails but is not limited to the following actions:

- **verifying the disclosed details against certain (public or private) databases (e.g. sanction lists,)**
- **ordering a credit report**
- **bank statement showing the initial deposit;**

If the Company is not able to verify the identity of the Player based on the provided documentation and further efforts, the Company reserves the right to put the Player Account on hold pending the provision of verification information, or to terminate the account if it finds the information contained in the Player Account to be false or misleading. Furthermore, the company engages in EDD to natural and legal entities, including financial institution in countries where the FTAF identified as a high-risk country.

3.2.3 Politically Exposed Persons

Situations involving PEP require the application of EDD measures, independently of the outcome of the risk assessment. This entails having to determine whether a Client is a PEP or otherwise and, should this be the case, apply of the following pre-established EDD measures:

- i. Obtain senior management approval to service the PEP;
- ii. Establish what is their source of wealth and, where applicable, their source of funds;
and
- iii. Conduct enhanced on-going monitoring of the Account Holder's activity.

Screening for PEP status has to be carried out regularly but it is important that this is done within thirty days of the EUR 2,000 threshold being met. Should an Account Holder who had not been identified as a PEP at on-boarding stage result to have become one, the Employee is required to carry out or implement the measures described in paragraph (i) to (iii) above within the thirty (30) day window, failing which he would have to terminate the business relationship with the said Account Holder.

Information required to determine whether an Account Holder (or its beneficial owner) is a PEP can be obtained either from the Account Holder himself (e.g. by completing a standardized self-declaration as to his status and, to the extent which may be applicable, that of his beneficial owner) or by using reliable electronic databases to screen their Account Holder database. However, where the Employee relies on the Account Holder to disclose and declare whether

he is a PEP or otherwise, he is required to (a) provide the Account Holder with guidance as to what is meant by a PEP, including by providing him with a definition of the said term; and (b) confirm on a risk sensitive basis the information so obtained.

3.2.4 Beneficial Ownership Identification & Verification

In compliance with Curaçao's AML/CFT regulations and international standards, the Company requires full disclosure and verification of beneficial ownership for all customer accounts held by legal entities or complex structures.

Definition of Beneficial Owner:

A beneficial owner is any natural person who:

- Directly or indirectly owns/controls 25% or more of a legal entity
- Exercises ultimate effective control over the account or entity
- Benefits from 25% or more of the property (for trusts/foundations)

Required Information:

For each beneficial owner, the Company collect and verify:

- Full legal name and date of birth
- Nationality and residential address
- Government-issued ID (passport/national ID number with copy)
- Nature and percentage of ownership/control
- Source of funds/wealth (for high-risk cases)

Verification Process:

- Obtain and review official documents (certificate of incorporation, shareholder register, trust deeds)
- Screen against sanctions/PEP lists
- Conduct ongoing monitoring for changes

Enhanced Due Diligence:

Applied when:

- Ownership structure is complex or opaque
- Beneficial owners are from high-risk jurisdictions
- PEPs are identified

3.2.5 The Risk Department

The Company has a designated risk department which is in charge of the review of KYC information and the monitoring of Player Account activities. Specifically, they are in charge of the following:

- Ensure a proper review of the Player Accounts by the personnel in relation to identification and verification of an Account Owner,
- Keep a list of registered Account Holders;
- Monitor the reviews and investigations conducted by the designated personnel performed on the Player Account activities;

- Provide initial and ongoing training to all relevant staff ensuring awareness of their personal responsibilities and the procedures in respect of identifying Players, monitoring Player activity, record-keeping and reporting any unusual/suspicious transactions;
- Cooperate with all relevant administrative, enforcement and judicial authorities in their endeavor to prevent and detect criminal activity;
- Ensure that this policy is adhered to, reviewed and maintained regularly.

3.3 The Monitoring of Account Holder activities

Designated personnel will conduct the reviews and the monitoring of the Player Accounts and will further conduct investigations in case any irregular activities are detected.

Security technologies are in place generating automated alerts which are thereafter thoroughly investigated by the department.

The presence of any irregular, suspicious, inappropriate or fraudulent activity or any attempt thereto, will cause the pertaining Player to be classified as High risk for which EDD procedures are implemented.

Player accounts are reviewed and monitored for the presence of any of the following situations:

- the provision of fake, false, incorrect, misleading, non-existing, KYC information which do not belong to the Player or are unable to be verified;
- provision of fictitious names such that the true beneficial owner is not known;
- the detection of inappropriate play and/ or fraudulent activity;
- the detection of irregular Player activity including but not limited to the placing of zero risk or even bets;
- complex or large transactions or groups of transactions which are likely, by their nature to be related to money laundering or the funding of terrorism;
- upon suspicion of a Player attempting to or having created multiple Player Accounts in multiple different names;
- upon suspicion of Player(s) being part of a syndicate of Players colluding to gain an advantage over the Company;
- at the detection of any irregular, suspicious, inappropriate or fraudulent activity by the Company's control systems;
- anytime, at the discretion of the Company;
- fraudulent or unlawful use of the system by Players, in an attempt to break into or otherwise circumvent the security measures set up by the system;
- The use of any software program endowed with Artificial Intelligence;
- Attempt to log in from a Non-reputable Jurisdiction.

Specific attention is paid to the following instances:

- **Multiple accounts**

Only one Player Account is permitted per person. If more than one Player Account is created per person, house, building, mailing address, phone number, IP address, family, Device or Shared Environment then all related Player Accounts be investigated and may be closed. No winnings, refund nor deposits will be paid out. Family includes, but is not limited to, parents, partners, spouse, children, siblings and close relatives.

If the suspicion arises that multiple Player Accounts have been created in multiple different names or that a Player Account is a part of a syndicate of Players colluding to gain an advantage over the Company, the Company will proceed to suspend all suspicious Player Accounts pending an investigation. The investigation will consist of the review of playing history, IP location histories including VPN and proxy databases and action to delay ratios commonly displayed with computer sharing technology. If the Company concludes from the investigation that an Account Holder or a group of Account Holders have created multiple accounts and are playing as part of a syndicate of Players, the Company will proceed to withhold any cash or bonus winnings and reserves the right to withhold deposited funds.

Whenever an Account Holder requests for a withdrawal of funds from his/ her account, the system will check the presence of multiple accounts and further checks whether the Account Holder has used a false proxy. At the presence of multiple accounts, all the accounts will be closed, and the Player Account will be denied the opening of a new account.

- **Identity fraud**

At the detection of any use of falsified documentation (identity fraud), the Company will proceed to close the Player Account(s). Any winnings arising from such activities shall be confiscated and the deposited amount will be subject to further investigation.

- **Unusual activities**

If an Account Holder has unusual deposits and gets flagged by the system, the Company will perform an investigation in which the Account Holder may be requested to provide further information. The Company will suspend the account until further documentation is in place. If the Player Account has not provided satisfying information within 30 days, the account will be terminated. The MLRO will proceed with the reporting of the unusual transaction to the relevant authority.

- **Withdrawal, deposit or pay out of funds**

All financial transactions must match the name of the credit card or other payment accounts through which the Player Account is funded, or money is withdrawn. Any inconsistencies will be considered a breach of the Terms and Conditions. The transaction will be suspended and the Player Account subject to further investigation.

The Company has established the following procedures with regards to the withdrawal, deposit or pay out of funds:

Deposits

A Player Account is only permitted to use its personal information and personal bank account. The information provided on the deposit form must be identical to the pertaining data held by the Company. An Account Holder may deposit money in his Player Account only in order to play on the Website and use the Services and is not allowed to withdraw without prior wagering activity. Furthermore, the Company will not grant interest on deposits. The Company reserves the right to apply certain restrictions to the payment methods in selected countries and/or for certain Players.

Request for withdrawal

Withdrawal requests must be made from a Player Account. Withdrawal requests sent by any other means of communication will not be processed. Upon receipt of a request for withdrawal, the Company will request KYC documentation verifying the identity of the Player, in accordance with its internal withdrawal process.

The Company will not deposit withdrawn funds to another source from which it was originated. If for any reason this is no longer possible, the Company will request additional verification documentation evidencing the details and ownership of the new withdrawal method. Transfers or pay outs will only be made to the Player. Transfers to third parties are not permitted.

- **Prior review of account activity**

Before processing any withdrawals, the Company will conduct additional review of the Player Account for any irregular activity such as money laundering or suspicious play such as:

- the placement of a deposit without having placed any bets, or only to receive free spins. A player must have always placed at least his deposit amount in bets before proceeding to withdraw the funds;
- the possible creation of multiple Player Accounts in multiple different names;
- possible collusion between Players, detected by the Company's fraud control system.

Upon the occurrence of any of the instances mentioned above, the Company may decide to withhold funds and proceed to further request EDD documentation or conduct further investigation and resolve to:

- suspend the Player Account until receipt of sufficient verification information, where still applicable;
- immediately block the access of a Player to the system or to his/ her account and seize all funds held in the account;
- close or terminate a Player Account and seize all funds held in such account,

Followed by the report of the activity to the relevant authority as further described below.

3.4 Transactions using Cryptocurrency

Cryptocurrency transactions are only possible if the initial deposit was made with a crypto currency. Following this transaction all transactions (deposits, wagers and payout) with the Player must be conducted using the same crypto currency as with the first deposit.

The Company will at no time sell/buy/exchange crypto currency with and/or to FIAT currency.

The Company is bound by the following requirements as set by the Master License Holder:

- Collect and verify proof of identity and proof of address as described above in the 'Client Due Diligence' paragraph and to make sure that the Player is over 18 years of age;
- Collection and storage of hardware KYC in all pathways from signup, login, deposits and withdrawals, including but not limited to IP address, mac address and browser information to ensure that all wagering, deposits and withdrawals are to/from the same Player (IP and computer);
- The Company will make available to the Master License holder on demand and provide proof of balance as acceptable by the Master License Holder, to ensure Player's funds have been deposited;
- Provide proof of Solvency to the Master License Holder on a periodic basis (weekly, monthly) to ensure that operator has all funds to cover all bets and jackpots and that the crypto currency is kept in a separate account.
- The Company will display the rate of exchange from crypto currencies to FIAT currency on the home page of the Website. In no way shall the Company make exchanges between any crypto currency and any FIAT currency.
- The Company must include in their Terms and Conditions and highlights that crypto currency values can change dramatically depending on the market value.

It is important to note that due to the current anti-money-laundering regulations, the Player may deposit money into the Player Account only in order to play and to use the Services. Likewise, the Player may only withdraw winnings and not the funds deposited into the Player Account. Players who deposit and withdraw without gaming activities will have their funds blocked until further notice. The Company is not a financial institution and does not grant interest on deposits. In any case, the Company reserves the unlimited right to apply certain restrictions to the payment methods in selected countries and/or for certain Players.

Notification of new payment methods will be made on the homepage of the Website and sent by e-mail to the Account Holders as they are added. For each new depositing method, this Manual and the Terms and Conditions on the Website will be updated accordingly.

4. Money Laundering Reporting Officer (MLRO)

The Company has designated an MLRO who is in charge of the review of KYC information and the monitoring of Player Account activities and is further assisted by designated personnel. The MLRO is in charge of the following:

- **ensure a proper review of the Player Accounts by the personnel in relation to identification and verification of an Account Holder,**
- **keep a list of registered Account Holders;**
- **monitor the reviews and investigations conducted by the designated personnel performed on the Player Account activities;**
- **provide initial and ongoing training to all relevant staff ensuring awareness of their personal responsibilities and the procedures in respect of identifying Players, monitoring Player activity, record-keeping and reporting any unusual/suspicious transactions;**
- **cooperate with all relevant administrative, enforcement and judicial authorities in their endeavor to prevent and detect criminal activity; and**
- **ensure that this policy is adhered to, reviewed and maintained regularly.**

4.1 Ongoing monitoring

The Company reserves the right to conduct a review at any time to validate the identity, age and/or registration data provided by the Player Account in order to verify the use by the Customer of the provided services for any breach of the Terms and Conditions and any applicable laws. At the moment of registration, the applicant provides the Company with authorization to make any relevant inquiries pertaining to his person and to use and disclose

information to any third party considered necessary in order to conduct its verification checks. Third party agencies may be engaged in an effort to confirm the provided age, identity, address and payment details, the ordering of a credit report and/ or the verification of the provided information by checking it against certain public or private databases. All applicants are made aware that by accepting the Terms and Conditions of the Company, they agree that the provided information may be used, recorded and disclosed and that the data may be recorded by the Company or third party engaged.

The review may be performed from time to time at the discretion of the Company and/or due to regulatory, security or other business reasons. During the review the Account Holder may be restricted from withdrawing funds from the Player Account and/ or prevented from accessing certain Services offered on the Website.

4.2 Reporting of unusual transactions

Any transactions or circumstances for which the Company has not received sufficient verifying information for and/or of which the Company knows, suspects or has reason to suspect that any of the transaction(s), among other actions, (i) involve funds derived from illegal activities, (ii) are intended to conceal funds from illegal activities, or (iii) involve the use of the Company system to facilitate criminal activity, may give rise to its report to the FIU. The Money Laundering Reporting Officer (MLRO) is in charge of the reporting with the relevant authority and will hold a list of all instances in which it did not consider it necessary to report. The decision not to report will be sufficiently supported. In case the report is filed with the FIU of Curacao or any internal investigation is taking place, the Account Holder shall not receive any of this information. It is prohibited to inform a Player or third parties of the reporting of or the intention to report an activity or transaction to the FIU.

4.3 Record keeping

The Company maintains a record of all relevant documentation on a separate database for at least five years after ending a business relationship. The Company is obliged to retain files in a way that enables investigating authorities to identify a satisfactory audit trail for individual transactions including the amounts, currencies and type of transactions.

In specific circumstances, if ordered by rule of law and permitted by national law and the relevant authorities, the Company may provide copies of the records maintained.

4.4 Training

In line to ensure the knowledge and awareness of the AML/CTF risks and the efforts conducted by the Company for the prevention thereof, all relevant staff are required to receive training at least once a year. The MLRO is responsible to determine the content of the training events but will ensure the following topics to be discussed:

- Awareness regarding certain topics and aspects concerning the fight, prevention, control and management of risks in relation to money laundering, the financing of terrorism and bribery and corruption amongst others;
- Policies and procedures maintained by the Company regarding the awareness, detection and deterrence of mentioned risks;
- Mechanisms, procedures, controls records and tools maintained by the Company in relation to the subjects discussed.

4.5 Staff Due Diligence & Whistleblower Protection

Staff Vetting Procedures

It is imperative that the Company's employees are of undisputed integrity. To ensure this objective, the Company follows a procedure whereby all applicants must produce a curriculum vitae, at least two references and relevant educational qualification certificates, and/or professional certificates, which are checked and verified by the Company's Human Resources Department.

Confidential Reporting Channels

We provide multiple secure avenues for reporting concerns:

- Encrypted webform with blockchain verification
- Dedicated compliance hotline with 24/7 multilingual support
- Direct access to the Chair of the Audit Committee

Whistleblower Protections

Good faith reporters are protected from retaliation under Curaçao law. All reports receive:

- Immediate confidentiality protections
- Independent investigation by the Compliance Oversight Team
- Formal resolution within 30 calendar days

Training Requirements

All personnel complete:

- Mandatory annual whistleblower policy training
- Quarterly awareness refreshers on reporting protocols
- Specialized training for management on handling disclosures

4.6 Periodical review of AML/CFT policies

The AML/CFT policies of the Company are subject to a yearly review, comprising of a fair and unbiased appraisal of each of the required elements of this policy. The review includes testing of internal controls and transactional systems and procedures to identify problems and weaknesses. The review may be conducted by Employee or group of Employees, so long as

the reviewer is not the MLRO and does not report directly to the MLRO.

5. Ongoing Monitoring Policy

Play UK Internet N.V. maintains an enhanced ongoing monitoring framework compliant with Curaçao's 2025 AML/CFT regulations and GCB Directive 2025-01. Our program includes:

5.1 AI-driven transaction monitoring with:

- Real-time behavioral analytics detecting play-to-laundry patterns
- Cross-platform aggregation of player activity (as mandated by 2025 GCB cross-operator reporting rules)

5.2 Dynamic risk reassessment:

- Continuous (rather than periodic) risk scoring using machine learning
- Automated triggers for EDD upon detection of:
 - Cryptocurrency transactions exceeding €1,000 (new 2025 threshold)
 - Cross-border transfers to/from high-risk jurisdictions
 - Any beneficial ownership change (now reported within 24 hours per 2025 rules)

5.3 Biometric verification checks:

- Quarterly facial recognition matching for high-risk accounts
- Liveness detection for withdrawals >€2,000 (2025 requirement)

6. Timing of Customer Due Diligence (2025 Regulations)

Play UK Internet N.V. implements CDD measures in accordance with Curaçao's 2025 AML Ordinance (Art. 7-9) and GCB Directive 2025-02, with the following mandatory timing requirements:

6.1 Initial CDD

- Before onboarding: Full identity verification (including biometric liveness check) for all players
- Before first deposit: Verification of:
 - Payment method ownership
 - Source of funds for transactions ≥€500 (reduced from €1,000)
 - Within 24 hours for:
 - Cryptocurrency deposits (per 2025 Virtual Asset Transfer Rule)
 - PEPs/high-risk customers (with temporary account restrictions until clearance)

6.2 Ongoing CDD

Continuous monitoring: AI-driven behavioral scoring triggers instant reviews for:

- Unusual gameplay patterns (e.g., rapid betting/cashing out)
- Mismatched device/IP locations

Scheduled reviews:

Risk Tier	Frequency (2025 Change)	New Requirements
High-risk	Real-time alerts + quarterly full review	Blockchain analysis for crypto players
Medium-risk	Monthly automated review + annual full CDD	Cross-check with new Curaçao Player Registry
Low-risk	Biannual automated review	Geo-tracking for jurisdiction compliance

6.3 Event-Triggered CDD

- Immediate re-verification required for:
- Transaction spikes: $\geq 200\%$ increase in 48h
- Account changes:
- New beneficial owner (reportable within 1 business day per 2025 Ownership Transparency Rule)
- Payment method changes
- VPN usage detection
- Regulatory alerts: Matches with Curaçao's 2025 Central Sanctions Feed
- Documentation Timeline
- All CDD records must be:
- Updated within 72 hours of triggering events (down from 7 days)
- Maintained for 7 years (extended from 5) with blockchain-based timestamps for crypto transactions

7. Reporting Obligations Under Curaçao's 2025 AML Regulations

Play UK Internet N.V. complies with the following enhanced reporting requirements under Curaçao's 2025 AML/CFT framework:

7.1 Suspicious Activity Reports (SARs)

Filing Deadline: 24 hours from detection (reduced from 48 hours in 2024)

Content Requirements:

- Must include blockchain hashes for crypto transactions
- Cross-referenced with Curaçao's new Central Player Registry IDs
- AI-generated risk scoring (per GCB Technical Standard 2025-04)

7.2 Threshold Transaction Reports

New Categories Reportable to FIU:

Transaction Type	Threshold	2025 Change
Crypto deposits	≥€500	(New)
Fiat withdrawals	≥€2,000/24h	(From €3K)
Cross-border transfers	Any amount	(Expanded)

7.3 Beneficial Ownership Updates

Within 1 business day of changes

Must include:

- Notarized proof of identity for new owners
- Wallet addresses for crypto-funded entities

7.4 Monthly Aggregate Reporting

New Digital Asset Activity Statement due by the 5th of each month showing:

- Total crypto/fiat conversion volumes
- Player geographic distribution
- SAR-to-transaction ratios

8. Termination of Business Relationship Policy

Play UK Internet N.V. complies with the following mandatory termination procedures under Curaçao's 2025 AML Ordinance (Article 32) and GCB Directive 2025-05:

8.1 Mandatory Termination Triggers

Business relationships must be terminated immediately (within 24 hours) for:

- Confirmed SAR Cases:
- Players linked to:
 - Terrorism financing (per UNSC Resolution 2462 updates)
 - Narcotics trafficking (new 2025 designated predicate offenses)

"Red Flag" Gaming Patterns:

- Chip dumping in peer-to-peer games
- AI-detected play-to-laundry behavior (≥3 alerts in 30 days)

Sanctions Matches:

- Appear on Curaçao 2025 Dynamic Sanctions List
- Use of OFAC-blocked crypto wallets

Material CDD Failures:

- Refusal to provide 2025-required biometric verification
- Beneficial ownership discrepancies (≥25% unreported)

8.2 Termination Protocol

Immediate Account Freeze:

- All player balances held for 14 days (extended from 7) for FIU review
- Crypto assets moved to cold wallet with regulatory hold

Notification Requirements:

To Player: Generic "compliance decision" notice (no specifics)

To Regulators:

- GCB Form T-2025 filed within 48 hours
- Full transaction history + AI risk scoring submitted via FIU's TERMINET portal

8.3 Prohibited Activities

No "Quiet Exits": All terminations must be reported (2025 Anti-Evasion Rule)
No Payouts until FIU clearance for:

- Transactions ≥€2,000 within 30 days pre-termination
- Crypto withdrawals to non-KYC'd wallets

8.4 Exceptions Process

Appeals: Players may submit evidence via GCB's Dispute Resolution Portal (72h response SLA)

Reinstatement: Only with:

- FIU's "No Objection" Certificate
- Fresh biometric KYC + €10,000 compliance bond (2025 requirement)

9. Reliance on Third Parties for AML Compliance

Play UK Internet N.V. may rely on third-party providers for customer due diligence (CDD) only when such parties are regulated entities (e.g., licensed financial institutions, registered VASPs, or approved gaming operators) that comply with Curaçao's 2025 AML Ordinance (Art. 12bis) and FATF Recommendation 17.

We ensure real-time access to original KYC data, conduct annual audits of third-party processes, and retain full accountability for AML compliance. All third-party relationships require pre-approval by our Compliance Officer and integration with our AI-driven monitoring systems to detect inconsistencies. Crypto-related verifications are permitted only with GCB-certified VASPs that adhere to the 2025 Travel Rule.

10. IT Security Measures for AML Compliance

Play UK Internet N.V. implements robust IT security measures to protect against data breaches and cyber threats in accordance with 2025 regulations.

- **Data Protection**
All customer data is encrypted using AES-256 standards. Transactions are secured with TLS 1.3 protocols. Crypto assets are stored in multi-signature wallets with blockchain monitoring.
- **Access Controls**
System access follows strict role-based permissions. Sensitive AML functions require dual authentication. High-risk actions need biometric verification.
- **Incident Response**
Our systems detect threats in real-time using AI monitoring. All breaches must be reported to the Curaçao FIU within 12 hours. Players are notified within 72 hours of confirmed incidents.
- **Compliance**
We use only GCB-approved vendors meeting ISO 27001:2025 standards. Annual penetration tests are conducted by certified cybersecurity firms. These measures ensure the integrity of our AML processes and protect customer information as required by 2025 regulations

Approved and signed by Managing Director of the Company.

Signature: _____

By: Mrs. Annemarie Heyer – Managing Director

Date of Approval:

Annex A

www.grandesloterias.com

www.playhugelottos.com

www.playusalotteries.com

www.lotto247.io