

PLAY UK INTERNET N.V.

AML MANUAL

Signature: *Annemarie Heyer*
Name: Annemarie Heyer, Managing Director
Date: June 4, 2026

V. 2.0 – June 2026

Table of Contents

REVISION HISTORY	4
DEFINITIONS AND ABBREVIATIONS.....	5
1. AML/CFT POLICY	9
1.1 POLICY.....	9
1.2 OBJECTIVES	10
1.3 SCOPE	10
2. REGULATORY FRAMEWORK	11
2.1 NATIONAL REGULATIONS.....	11
2.2 INTERNATIONAL REGULATIONS	12
3. PROCEDURES	12
3.1 RISK MANAGEMENT.....	12
3.1.1 <i>Risk assessment</i>	13
3.2 CLIENT ACCEPTANCE PROCEDURE	23
3.2.1 <i>Client Risk Classification</i>	23
3.2.2 <i>Know Your Customer Procedure</i>	24
3.2.3 <i>Due Diligence</i>	24
3.2.4 <i>High risk Individuals</i>	28
3.3 THE MONITORING OF ACCOUNT HOLDER ACTIVITIES	30
3.3.1 <i>Unusual activities</i>	30
3.3.2 <i>Deposits and Withdrawals</i>	30
3.3.3 <i>Transactions using Cryptocurrency</i>	32
3.3.4 <i>Ongoing monitoring</i>	33
3.4 REPORTING OF UNUSUAL TRANSACTIONS.....	33
3.4.1 <i>Internal Unusual Activity Reporting</i>	35
3.4.2 <i>External Unusual Activity Reporting</i>	35
3.5 RECORDKEEPING.....	36
4. THE COMPLIANCE FUNCTION (CF)	37
5. TRAINING	38
6. STAFF DUE DILIGENCE	38
7. PERIODICAL REVIEW OF AML/CFT POLICIES.....	38
8. EXAMINATION BY THE GAMING CONTROL BOARD	39

CONTACT INFORMATION	39
---------------------------	----

REVISION HISTORY

Version #	Effective Date	Approving Official	Responsible Office	Next Review Date	Comments
1.0	May 26, 2025	eMoore N.V.	Compliance function	May 26, 2026	-
2.0	May 30, 2026	eMoore N.V.	Compliance function	May 30, 2027	-

Definitions and Abbreviations

Account Holder	An individual who has a Player Account on the Website.
Anti Money Laundering (“AML”)	All efforts focused on the prevention of money laundering, the direct or indirect participation in any transaction that seeks to conceal or disguise the nature or origin of funds derived from illegal activities.
Caribbean Financial Action Task Force (“CFATF”)	An organization of states and territories of the Caribbean territory that have agreed to implement common countermeasures against money laundering and terrorism financing. (www.cfatf-gafic.org)
Combatting terrorist financing (“CFT”)	All efforts focused on the prevention of providing funds at the disposal of terrorists to be used for committing terrorist attacks.
Combatting proliferation of weapons of mass destruction (“CPWMD”)	Efforts aimed at combatting the financing or provision of funds for the sale, transfer, or export of nuclear, chemical or biological weapons, their delivery systems and related materials.
Compliance Officer (“CO”)	Designated individual in charge of the review of KYC information and the monitoring of Player Account activities. The CO might further be assisted by designated personnel.
Cryptocurrency	Distributed, open-source, mathematically based peer-to-peer virtual currencies that have no central administering authority, and no central monitoring or oversight. Examples include Bitcoin, Ethereum, Litecoin and Dogecoin.
Cryptocurrency transaction	The deposit and withdraw of cryptocurrencies into and out of a Player Account held by a Player.
The Company	PLAY UK INTERNET N.V., a limited liability company duly organized under Curaçao law registered with the Chamber of Commerce and Industry in Curaçao under number 95091.

Employee	Any person working for the Company.
Financial Action Task Force ("FATF")	An intergovernmental organization dedicated to developing standards and promoting effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. (www.fatf-gafi.org)
Financial Intelligence Unit ("FIU")	Pursuant to FATF Recommendation no. 26, countries must establish a Financial Intelligence Unit (FIU) that serves as a national center for the receiving (and, as permitted, requesting), analysis and dissemination of suspicious transaction reports (STR) and other information regarding potential money laundering or terrorist financing.
Know Your Customer ("KYC")	Know Your Customer, the mandatory process of identifying and verifying the customer's identity when opening a Player Account and periodically over time.
Money Laundering ("ML")	A process through which criminals conceal, or attempt to conceal, the origin of the proceeds of their illegal activities and disguise, or attempt to disguise, such proceeds to make them appear to be legitimate.
Player	Individual who has registered with the Company for the purpose of making use of the Services offered on the Website and for which a Player Account has been opened providing him/her with a unique code.
Player Account	An account granted to an individual after registration on the Website. The Player 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 IP address, per family and per Shared Environment.
Politically Exposed Person ("PEP")	A person entrusted with a prominent public function, such as a senior political figure. Individuals closely related to this person, for instance immediate family members and close associates, are also considered PEPs. PEPs are classified as a Money Laundering risk since they may be exposed to property that has been

	generated by corruption and bribery because of their position.
Restricted Jurisdictions	Jurisdictions that are restricted either under the Curaçao license conditions by the Curaçao Gaming Authority at a certain moment, or by decision of the Company's managing director at a certain moment when and where still applicable, as well as countries mentioned on the FATF blacklist or on which any financial sanctions has been imposed by the EU/ U.N. and/or the OFAC. List of restricted jurisdictions: Games and services will not be rendered in the following countries: United States of America and all its dependencies territories and its minor outlying islands, United Kingdom, Spain, France, Netherlands, Curaçao and Australia. In addition, in accordance with local regulatory requirements, game provider restrictions, and contractual obligations, certain individual games or categories of games may be restricted or prohibited in other jurisdictions. Such game-specific restrictions: - are determined and described in the Company's Terms and Conditions and/or related product documentation; - are updated on an ongoing basis; and - are not exhaustive.
Proliferation Financing ("PF")	The act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.
the Regulator	The Curaçao Gaming Authority (CGA). The regulator for the entire gaming industry operating in and from Curaçao.

Sanctions	Sanctions refer to restrictive measures imposed by international, regional, or national authorities to maintain or restore international peace and security, prevent terrorism, combat money laundering, proliferation financing, and serious human rights violations. Sanctions may include, but are not limited to: financial restrictions, including asset freezes and prohibitions on making funds or economic resources available; trade and economic embargoes; restrictions on the provision of services. For the purposes of this Policy, sanctions include measures imposed by: The United Nations Security Council (UNSC); The European Union (EU); United Kingdom; The United States Office of Foreign Assets Control (OFAC), where applicable; and any other competent authority recognized by the Curaçao Gaming Authority or applicable law noting the national legislation i.e. the Sanctions National ordinance and the Kingdom Sanction Act.
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 offices. Only one Player Account is permitted per Shared Environment.
Service	the gaming and betting offers provided by the internet gateway operated by the Company to the Account Holder, through the Website.
Terms and Conditions	The terms and conditions for the use of the Services, as published on the Website.
Terrorism Financing ("TF")	The process of making funds or other assets available to terrorist groups or individual terrorists to support them, even indirectly, in carrying out terrorist activities.
Website	the online gaming platform offering online gaming services 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, requiring all vulnerable sectors to implement appropriate safeguards for the prevention of their misuse for these purposes. Individuals involved in ML and/or TF continually attempt to exploit services and products to conceal their unlawful activities and proceeds' true nature. Such illicit activities must be identified promptly and mitigated through effective controls. AML policies incorporate regulations and laws for limiting financial criminals from concealing funds collected through illicit sources.

Money laundering in the online gaming industry typically manifests in two primary 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 signification 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.

The Company takes AML/CFT/CPF compliance 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 Objectives

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, CFT and CPF obligations based on national and international regulations;
- e) maintain appropriate records to support supervisory and regulatory oversight.

1.3 Scope

This Policy applies to all persons working for the Company or on the Company's behalf in any capacity, including 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

National regulations covering AML/TF/PF as well as the Curaçao gaming sector, as applicable to the Company are the following:

- a) The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- b) The National Ordinance on Money Laundering (P.B. 1993, no. 52);
- c) 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;
- d) The National Ordinance on Identification of Clients when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2024 no.41 (N.G. 2017, no. 99)) (NOIS) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- e) The National Ordinance on Games of Chance (LOK) (N.G. 2027, no. 157)
- f) 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);
- g) Sanctions national decree Al-Qaida c.s., the Taliban of Afghanistan c.s. Osama bin Laden c.s., and terrorist to be designated locally (N.G. 2010, no. 93); and
- h) 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.
- i) National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- j) Sanctions National Ordinance (N.G. 2014, no. 55)
- k) Kingdom Sanction Act (N.G. 2016, no. 54);
- l) Policies and Guidelines issued by the Curaçao Gaming Authority.

These laws and decrees underpin Curaçao's financial sector safeguards against money laundering, terrorism financing, and other crimes, while the CGA regulatory instruments serve to ensure fair, responsible, and corruption-free gaming, strengthening the industry overall.

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 an international level, the FATF plays an important role in the combating of ML, TF and PF. The FATF monitors the progress of its members in implementing necessary measures, reviews ML and TF techniques and countermeasures, 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 when providing Services to Account Holders. These procedures cover the following standards:

- Risk management
- Know Your Customer Procedure
- Monitoring of Account Holder activities
- Reporting of unusual transactions
- Recordkeeping

3.1 Risk Management

The Company applies a risk-based approach (RBA) in accordance with FATF Recommendations.

This approach requires the Company to identify, assess, and understand the ML/TF/PF risks to which it is exposed and to apply mitigation measures that are proportionate to those risks.

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

- i. identifying the ML and TF risks relevant to the Company through established sources and expert input;
- 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. review and update risk assessments periodically or upon material changes.

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

3.1.1 Risk assessment

The possibility of online gaming being used by criminals to assist ML 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 conducted a comprehensive Business risk assessment to identify its risks and manage them accordingly. In line herewith, further specific procedures are drawn up to further describe the processes that need to be in place.

3.1.1.1 Bussiness risk assessment

The Company assessed its risks by identifying, categorizing, and evaluating their likelihood and impact, and then calculated the inherent risk score using a standardized method. Applicable mitigation strategies and associated controls have then been mapped along with the assessed control effectiveness. The derived residual risk and corresponing risk level is further determined and categorized by aligning the risk thresholds with organizational risk appetite. This approach ensures consistency, transparency, while enabling prioritization of risks requiring additional action, while supporting ongoing monitoring and periodic reassessment.

Calculation:

- **Inherent risk:** The level of risk present in the business before any controls, mitigations or safeguards are applied.

The Company maintains its calculation as the product of likelihood and impact. A scale of 1 – 5 is used for scoring.

Inherent risk = Likelihood x Impact

- **Likelihood:** (L) The probability that a customer will engage in behaviour associated with financial crime risk.

Scoring scales:

- 1 – Rare – Highly unlikely to occur
- 2 – Unlikely – Could occur, but not expected under normal conditions
- 3 – Possible – May occur occasionally
- 4 – Likely – Expected to occur in most circumstances
- 5 – Almost certain – Occurs frequently or is inevitable

- **Impact:** (I) The potential severity of regulatory, financial, or reputational consequences arising from such behaviour.

Scoring scales:

- 1 – Insignificant – Minimal impact; no disruption to operations
- 2 – Minor – Limited impact; manageable within routine processes
- 3 – Moderate – Noticeable disruption; requires management attention
- 4 – Major – Significant impact; affects key objectives or performance
- 5 – Severe / Critical – Critical impact; threatens business continuity or viability

- **Inherent Risk score**

Scoring range:

- 1-5 – Low – Acceptable risk; minimal monitoring required
- 6-10 – Medium – Manageable risk; mitigation should be considered
- 11-25 – High – Significant risk; mitigation required and monitored closely or immediate required action is to be taken

- **Residual risk:** the exposure that remains after all reasonable management measures, safeguards, and controls have been implemented to mitigate an identified risk.

Control effectiveness is further factored in using a subtraction method, where the mitigation effectiveness control score is deducted from the inherent risk score to determine the residual risk. A minimum floor (1) is applied to ensure that risk is never fully eliminated.

- **Residual risk = Inherent risk – mitigation control score**

A residual risk matrix further portrays the residual risk after mitigating controls, supported by a legend defining severity levels and scoring bands. The scoring interpretation is same as displayed in the inherent Risk score above.

Business Risk Assessment

The following tables display the risk management of the identified risks the Company is exposed to, the likelihood, impact and calculated risk score.

Risk ID	Risk	Risk Category	Likelihood	Impact	Risk score (LxI)
R001	Breach of licensing terms in any jurisdiction	Regulatory & legal	4	5	20
R002	Failure to comply with AML/CTF regulations	Regulatory & legal	5	5	25
R003	Non-compliance with responsible gambling regulations	Regulatory & legal	4	4	16
R004	Advertising violations	Regulatory & legal	3	4	12
R005	High player payout rates reducing profit margins	Financial	3	4	12
R006	Cash flow liquidity issues	Financial	4	5	20
R007	Fraudulent chargebacks	Financial	4	3	12
R008	DDoS attack disrupting platform access	Cybersecurity	3	5	15
R009	Data breach or data loss	Cybersecurity	4	5	20
R010	Unauthorized access to customer data	Cybersecurity	3	5	15
R011	System outages or downtime during peak events	Operational	3	5	15
R012	Dependence on third-party software or platforms	Operational	4	3	12
R013	Poor internal controls over betting limits or bonuses	Operational	2	4	8
R014	Entry of a dominant competitor in key market	Market	4	4	16
R015	Decline in consumer trust in online	Market	3	5	15

	gambling				
R016	Reduced customer retention	Market	3	4	12
R017	Negative media coverage or scandals	Reputation	4	5	20
R018	Social responsibility criticisms	Reputation	3	4	12
R019	Players developing gambling addiction	Responsible Gambling	3	5	15
R020	Failure to intervene with at-risk players	Responsible Gambling	2	4	8
R021	Poor performance of software vendors	Vendor	3	4	12
R022	Payment processor instability or failure	Vendor	4	4	16

Mitigation strategy

This tables presents the mitigation strategy to be implemented, the effectivity rate, the activities to reduce residual risk, the residual risk score. Residual risks are classified into Low, Medium, or High categories enabling clear prioritization and reporting. A heatmap is provided as well showing the pertaining residual risk level.

Risk ID	Mitigation Strategy	Mitigation control effectiveness
R001	Regular audits, engage local counsel	12
R002	Automated monitoring tools, staff training	15
R003	Self-exclusion tools, RG team	10
R004	Ad approval workflow, legal review	7
R005	Game RTP analysis, betting limits	7
R006	Liquidity reserves, cash forecasting	12
R007	Payment verification systems, fraud detection software	7
R008	Cloudflare, WAF, redundancy	9
R009	Encryption, multi-layer security	12
R010	Role-based access control, 2FA	9
R011	Load testing, cloud infrastructure	9
R012	SLA enforcement, redundancy plans	7
R013	Control dashboards, alerts	5
R014	Brand differentiation, loyalty programs	10
R015	Transparency campaigns, PR management	9
R016	Personalized offers, CRM automation	7
R017	Crisis communication plan	12
R018	Fund RG programs, public reports	7
R019	Monitoring, self-exclusion tools	9
R020	Behavior tracking algorithms	5
R021	Performance KPIs, backup vendors	7
R022	Multiple PSPs, weekly performance review	10

Risk ID	Activities to reduce Residual risk	Risk score (LxI)	Mitigation control effectiveness	Residual risk score	Residual risk level
R001	Continuous license compliance training, implement internal reviews	20	12	8	Medium
R002	Enhance KYC processes, deploy AI for transaction monitoring	25	15	10	Medium
R003	Audit RG tools quarterly, include customer feedback	16	10	6	Medium
R004	Implement retention journeys, feedback loops with frequent users	12	7	5	Low
R005	Build trust with player protection features, transparency dashboards	12	7	5	Low
R006	Introduce real-time liquidity dashboards, diversify revenue streams	20	12	8	Medium
R007	Analyze competitor promotions, improve personalization engine	12	7	5	Low
R008	Set up DDoS scrubbing service, automate scaling responses	15	9	6	Medium
R009	Conduct periodic penetration testing, enforce data classification policies	20	12	8	Medium
R010	Apply anomaly detection for access patterns, monitor admin activities	15	9	6	Medium
R011	Use high-availability architecture, incident response planning	15	9	6	Medium
R012	Use player interaction scoring, initiate guided interventions	12	7	5	Low
R013	Implement regular vendor reviews, renegotiate SLAs	8	5	3	Low
R014	Perform market SWOT analysis, adjust promotional strategies	16	10	6	Medium
R015	Assess vendor dependency, contractual penalties for downtime	15	9	6	Medium
R016	Develop reputation resilience strategy, engage media consultants	12	7	5	Low
R017	Media monitoring, train spokespersons, prepare PR statements	20	12	8	Medium
R018	Fund responsible gambling campaigns, issue public responsibility reports	12	7	5	Low
R019	Install automated alert systems, limit manual overrides	15	9	6	Medium
R020	Perform regular PSP reliability audits, diversify payment options	8	5	3	Low
R021	Automate detection of addictive behaviors, player nudges	12	7	5	Low
R022	Onboard backup payment partners, conduct stress tests	16	10	6	Medium

Likelihood\ Impact

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Legend

Low	1-5
Medium	6-14
High	15-25

The model is deliberately designed without complex weighting or percentage adjustments to promote transparency, and ease of use while ensuring results remain traceable and reproducible.

The Company is in the process to develop technological development risk assessment procedures for new products, payment methods, and delivery channels which should be regarded as an addition to this policy.

3.1.1.2 Customer Risk Assessment (CRA)

The Customer Risk Assessment (CRA) is conducted to determine the level of ML/TF/PF risk associated with each customer and to ensure that appropriate Customer Due Diligence measures are applied.

The CRA shall be performed:

- Prior to establishing a business relationship; and
- On an ongoing basis throughout the lifecycle of the relationship.

Risk areas

The Customer Risk Assessment covers four areas:

- Customer risk including player activities
- Product/Service (game type),
- Transaction risk (funding methods),

- Interface risk, and
- Geographical risk.

Customer risk

Customer risk refers to the risk of money laundering and terrorist financing arising from establishing or maintaining a business relationship with a customer, which may vary depending on the customer's type and characteristics. This assessment of the risk by a player is generally based on the person's economic activity and/or source of wealth.

Product/ Services, and transaction risk

Product, service, and Transaction risk refers to products, services or transactions that are more susceptible to criminal exploitation. This includes gaming products or services that allow customers to influence game outcomes, whether acting alone or collusion with other participants.

The use by players of specific funding methods, which are considered to resent a higher risk of ML/TF, are also treated as high risk factors.

Interface risk

The method used to establish a business relationship or conduct transactions can affect the risk level. Methods that favor anonymity increase the risk of ML/TF if no measures are taken to address the risk.

Geographical risk

The geographical risk is the risk posed to the Company by the geographical location of the business/ economic activity and the source of wealth/funds of the business relationship.

A customer's nationality, country of residence, and place of birth should be taken into account as these elements may signal exposure to heightened geographical risk.

Jurisdictions with deficiencies in their AML/CFT regimes, significant corruption concerns, exposure to international sanctions linked to terrorism or the proliferation of weapons of mass destruction, or known terrorist activity should be regarded as high risk. Jurisdictions lacking such risk factors may be classified as medium or low risk for ML/TF purposes.

Calculation

A consistent and transparent scoring framework is used to enable reliable and auditable risk assessment.

As with the Business Risk Assessment, the Inherent risk is calculated by multiplying Likelihood and Impact on a standard scale of 1 to 5, generating a score from 1 to 25 that reflects the risk's initial severity prior to the application of any controls. The same calculation methods are used.

▪ **Inherent risk – Likelihood x Impact**

Likelihood (L): the probability or frequency that a specific risk event will occur within the business environment in relation to the player e.g. player behavior, High-risk channels exposure.

Impact (I): represents the severity of the consequences if the risk event materializes. The model considers for example Reputational damage and Operational disruption

Inherent risk: risk that exists in the absence of any controls or mitigation measures when servicing customers

▪ **Residual risk = Inherent risk – mitigation control score**

A residual risk matrix further displays the residual risk after mitigating controls, supported by a legend defining severity levels and scoring bands. The scoring interpretation is same as displayed in the inherent Risk score above.

As with the BRA, residual risks are classified into Low, Medium, or High categories to support clear prioritization and reporting. The model is deliberately designed without complex weighting or percentage adjustments to promote transparency, and ease of use while ensuring results remain traceable and reproducible.

Customer Risk Assessment

The following tables display the risk management of possible customer risk it is exposed to, the likelihood, impact and calculated risk score.

Risk ID	Risk Category	Risk	Likelihood	Impact	Inherent Risk (LxI)
CR001	Customer Risk	Use of prepaid/gift cards	3	4	12
CR002	Customer Risk	Use of VPN/proxy masking location	4	4	16
CR003	Customer Risk	Onboarding of Politically Exposed Persons (PEPs)	3	5	15
CR004	Customer Risk	High spenders without clear source of income	3	4	12
CR005	Customer Risk	Anonymous behaviour	4	4	16
CR006	Customer Risk	False identity or incomplete customer KYC	5	5	25
CR007	Customer Risk	Use of cryptocurrency for deposits	3	5	15
CR008	Customer Risk	Structuring/unusual transaction behaviour	4	5	20

CR009	Customer Risk	Multiple linked accounts	3	4	12
CR010	Customer Risk	Customers from high-risk jurisdictions	3	5	15
CR011	Customer Risk	Self-excluded individuals re-registering	2	3	6
CR012	Customer Risk	Frequent chargebacks/disputes	3	4	12
CR013	Customer Risk	Account takeover indicators	3	5	15
CR014	Customer Risk	Use of third parties or accounts from others	4	4	16
CR015	Customer Risk	Nature of income: multiple or irregular income streams	4	4	16
CR016	Funding Method	Debit/credit cards	3	3	9
CR017	Funding Method	Licensed PSPs	3	3	9
CR018	Funding Method	PSPs funded with cash/quasi-cash	5	5	25
CR019	Funding Method	Prepaid cards/vouchers	5	5	25
CR020	Funding Method	Bank transfers (regulated jurisdictions)	2	3	6
CR021	Game Type	Fixed odds games without hedging (slots, lotteries)	5	3	15
CR022	Game Type	Fixed odds games with hedging (blackjack, roulette)	3	4	12
CR023	Game Type	Sports betting	5	5	25
CR024	Game Type	P2P games (poker)	5	5	25
CR025	Geographical Risk	High-risk jurisdictions (FATF list/OFAC/EU sanctions)	5	5	25
CR026	Geographical Risk	VPN/proxy usage	5	5	25
CR027	Interface Risk	Remote automated registration	5	5	25
CR028	Interface Risk	Registration via intermediary	3	4	12
CR029	Interface Risk	Master account structures	5	5	25
CR030	Transaction Risk	High-value deposits or spending patterns	5	5	25

Mitigation strategy and residual risk towards AML risk

The following tables show the mitigation strategy to be implemented and the effectivity rate.

Risk ID	Mitigation Strategy	Mitigation control effectiveness score
CR001	Restrict usage; apply EDD thresholds	7
CR002	Device fingerprinting; additional KYC; detect VPNs;	10
CR003	PEP screening, EDD, senior management approval, continuous monitoring; SOF/SOW checks;	9
CR004	Income verification; affordability checks	7
CR005	Tiered onboarding; ID verification; biometrics	10
CR006	KYC procedures, document verification, biometric checks, ongoing monitoring	5
CR007	Wallet KYC; blockchain analytics; transaction limits	12
CR008	Real-time transaction monitoring; behavioral alerts	12
CR009	Device fingerprinting; IP monitoring, account linkage detection, account restrictions	8
CR010	Geo-blocking; EDD; risk profiling	9
CR011	Shared exclusion lists; ID verification; monitoring	3
CR012	Limit refunds; monitor payment patterns	7
CR013	Behavioral analytics; device alerts; step-up authentication	9
CR014	Identity verification, monitoring unusual patterns, restrict third-party transactions	3
CR015	Enhanced due diligence (EDD), request source of funds verification, ongoing monitoring	3
CR016	3DS authentication; cardholder verification; fraud monitoring	15

CR017	PSP due diligence; transaction monitoring by provider tier	12
CR018	EDD; transaction caps; proof of funds requirements	9
CR019	Deposit limits; restrict withdrawals; enhanced monitoring	6
CR020	KYC matching; source of funds checks; reliance on banking	15
CR021	Monitor rapid deposit/play/withdraw cycles; wagering requirements; low gameplay turnover alerts	9
CR022	Detect structured betting; limit table switching; behavioral analytics	9
CR023	Monitor arbitrage and unusual betting; integrity feeds; linked account detection	9
CR024	Collusion detection; chip dumping monitoring; player network analysis	9
CR025	Geo-blocking; sanctions screening; enhanced due diligence	12
CR026	IP intelligence, IP/VPN block; location mismatch alerts; detect VPNs	10
CR027	eKYC; biometric verification; liveness detection; device fingerprinting	9
CR028	Intermediary due diligence; audit trails; linked account monitoring	9
CR029	Restrict/prohibit; beneficial ownership transparency; account segregation	6
CR030	Transaction monitoring systems with alerts, threshold-based reviews, manual investigations	5

The following table displays the activities to be conducted to reduce residual risk. The residual risk score is provided as well as the residual risk level with corresponding heatmap.

Risk ID	Activities to reduce Residual risk	Inherent Risk (LxI)	Mitigation control effectiveness score	Residual risk score	Residual risk level
CR001	Restrict anonymous usage; BIN monitoring; transaction caps	12	7	5	Low
CR002	IP intelligence; GPS mismatch detection; step-up authentication	16	10	6	Medium
CR003	Enhanced adverse media checks; periodic PEP re-screening	15	9	6	Medium
CR004	Open banking verification; income-spend ratio monitoring	12	7	5	Low
CR005	Behavioral biometrics; progressive profiling	16	10	6	Medium
CR006	Multi-source verification; video KYC; AI document forensics	25	5	20	High
CR007	Blockchain intelligence expansion; wallet clustering analysis	15	12	3	Low
CR008	ML anomaly detection; aggregation rules; peer analysis	20	12	8	Medium
CR009	Graph analytics; shared credential detection	12	8	4	Low
CR010	Dynamic geo-risk scoring; cross-border monitoring	15	9	6	Medium
CR011	Biometric matching; shared exclusion databases	6	3	3	Low
CR012	Merchant descriptor monitoring; dispute pattern analytics	12	7	5	Low
CR013	Session monitoring; behavioral anomaly detection	15	9	6	Medium
CR014	Strict name matching; restrict third-party transactions	16	3	13	High
CR015	Open banking checks; affordability modelling	16	3	13	High
CR016	Tokenization; enhanced fraud scoring	9	15	1*	Low
CR017	Ongoing PSP monitoring; SLA-based risk reviews	9	12	1*	Low
CR018	PSP audits; source-of-funds validation	25	9	16	High
CR019	Restrict anonymous cards; cooling-off periods; BIN blocking	25	6	19	High
CR020	Payment reconciliation; beneficiary verification	6	15	1*	Low
CR021	Gameplay analytics; abnormal play detection	15	9	6	Medium
CR022	Bet pattern modelling; limit switching detection	12	9	3	Low
CR023	Integrity feeds; arbitrage detection; exposure limits	25	9	16	High

CR024	Collusion detection; network analysis	25	9	16	High
CR025	Sanctions screening; transaction geo-filtering	25	12	13	High
CR026	Proxy detection; TOR blocking; IP reputation scoring	25	10	15	High
CR027	Bot detection; liveness checks; device fingerprinting	25	9	16	High
CR028	Intermediary audits; traceability controls	12	9	3	Low
CR029	UBO transparency; restrict pooled accounts	25	6	19	High
CR030	Dynamic thresholds; velocity rules; manual review triggers	25	5	20	High

CRA Residual Risk Matrix

Likelihood \ Impact

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Legend

Low	1-5
Medium	6-10
Critical	11-25

3.2 Client Acceptance Procedure

The Company has set standards determining whether a prospective customer can be accepted as a customer. These standards are based on Curaçao's AML legislation and international best practices. The acceptance of an applicant will be determined through proper establishment of the identity and verification thereof, the assessment of their profile and ensuring they meet all regulatory, legal and internal standards that align with the Company's risk appetite.

3.2.1 Client Risk Classification

Upon registration, the Company makes a provisional risk classification based on the initially collected information. A proper level of Customer Due Diligence (CDD) can then be applied for each Account Holder/customer.

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.

3.2.2 Know Your Customer Procedure

To register for a Player Account, an applicant must register personally and provide the following information:

- a. First and last name;
- b. Date of birth;
- c. Place of birth;
- d. Permanent residential address;
- e. Nationality;
- f. ID card number
- g. Valid email address and
- h. Username and a password.

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.

The verification of the identity entails validating the personal details obtained for identification purposes through reliable and independent source documents, data or information.

The type and extent of documentation required for verification will depend on the assigned risk.

3.2.3 Customer Due Diligence

The Company applies Customer Due Diligence measures in accordance with the risk-based approach. The extent and nature of CDD measures shall be determined by the level of risk identified.

CDD measures include primarily:

- The identification of customers and verification of the identity using reliable, independent source documents, data, or information; and
- Conducting ongoing monitoring establishing the understanding of the purpose and intended nature of the player.

Only natural persons are accepted as customer. No establishment of the identify of beneficial owner is in place. At all times identification can be requested establishing the identity of the Player.

The Company applies customer due diligence measures on a risk-sensitive basis. Simplified, Standard or Enhanced due diligence measures are applied in direct proportion to the level of money laundering and terrorist financing risk identified at onboarding following the Customer Risk Assessment and following the Account Holder activity on the platform, if required

3.2.3.1 Simplified Due Diligence

Simplified Due Diligence is conducted at account opening, in low risk scenarios. The Company will request the information as indicated in Section 3.2.2 above.

Verification will be conducted through the request of reliable, independent source documents, data or information. The Company requests:

- The copy of a valid passport document;
- Copy of a valid Identity card;
- Copy of a utility bill or bank statement.

Verification of identity is conducted at any time following the account opening but in any case, upon reaching the threshold of XCG 4.000 or the equivalent thereof.

3.2.3.2 Standard Due Diligence

Standard Due Diligence is applied by default to applicants who have been assigned a medium risk, or players who do not meet the criteria for enhanced measures; in any case in the following situations:

- i. anytime during the Player onboarding;
- ii. upon a request for withdrawal; and
- iii. anytime at the discretion of the Company.
- iv. When a transaction or incidental transaction of XCG 4.000 or more takes place.

All applicants are required to submit proof of identity, proof of address and payment ID at moment of deposit of funds or where applicable at any given time requested by the Company. Account holders are required to submit satisfactory documentation to proof the identity and residential address including but not limited to copies of:

- a. valid passport;
- b. identity card;
- c. driving license; and/or

- d. recent utility bill not older than three months.

Depending on the method used for the verification of the authenticity of the documentation, the documents are not required to be certified prior to the provision thereof. Further specifications in relation to the method of verification are to be detailed in separate complementary instruments to this document. In case the Company discovers that a transaction in the course of the business relationship of an amount of XCG 4.000 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. If requested information is not received within 30 days from the moment the threshold was reached, the Company will close the account and report the transaction to the FIU if a presumption of ML or TF exists. The CO will determine whether the funds will be blocked or not. In case of no such suspicion, funds held on the account will be transferred to the same bank account or wallet it was deposited from.

The Company will proceed to review the information provided within a reasonable time and will contact the applicant and request further information in case the documentation provided is found to be unsatisfactory. A document may be considered unsatisfactory if it is not in English, is suspected to be fraudulent, is suspected to be obtained from a third party to perform illegal operations over the Internet, or for any other reason subject to the discretion of the Company. The applicant may be required to provide further information or information in the internationally accepted format, including but not limited to requesting official translation of legal documents with appropriate seals. If the applicant does not succeed in providing sufficient information, refuses to do so or provides documentation not meeting the criteria (e.g. forged, altered, failing security checks), the Company may immediately proceed to permanently close the Player Account without the refund of the deposited amount.

3.2.3.3 Enhanced Due Diligence

Enhanced Due Diligence is applied in situations where a higher money laundering, terrorist financing, or proliferation financing risk is perceived, anytime during onboarding; during the monitoring of Account Holder activities; or at the discretion of the Company. These situations include but are not limited to:

- Politically Exposed Persons (PEPs)
- Customers from high-risk jurisdictions;
- unusual transaction patterns;

EDD measures include:

- obtaining senior management approval prior to establishing or continuing the relationship;
- taking reasonable measures to establish the source of wealth and source of funds;
- Conducting enhanced ongoing monitoring.

Due diligence measures are adjusted where risk levels change.

If 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;
- request to provide information/ documentation showing source of funds/wealth.

The Company reserves the right to restrict the Account Holder from withdrawing funds from the account and/or prevent access to all or certain parts of the services.

Failure to pass the checks may result in permanent closure of the Player Account and suspension of any of the outstanding balance

The Residual risk level further determines the monitoring frequency of the relevant Player and its activities on the platform. For example:

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)

3.2.4 High risk Individuals

The Company has determined the following customer categories to represent a high and or higher than average risk of ML/TF/FP. Depending on the risk, the Company can decide to reject the application or close the account in case any of these instances is identified after having accepted the individual as a client:

- Minors

An individual cannot make use of the Services unless that individual is over eighteen (18) years of age or any legal age at which gambling or gaming activities are permitted under the law or jurisdiction applicable to his person. No account will be opened for an underage individual permitting minors to (a) open an account for wagering and depositing fiat or crypto; nor to (b) to wager in fiat, crypto or on credit.

- Anonymous accounts

At registration an individual is required to provide his/her full name as well as further personal information. It is impossible to open an account without providing personal information.

The individual can only play on their own behalf, not for other individuals nor for legal persons.

- Corporate Accounts

Corporate Accounts, operated by companies, partnerships, trust or any other type of legal entity or structure or multi-funded arrangements are not accepted. Registration is only accessible for natural persons. This reduces the risk exposure due to e.g. eliminating complex tasks of identifying the true beneficial ownership or controlling parties, or minimizes the regulatory risk of dealing with shell companies.

- Sanctioned individuals

The Company screens all applicants against international sanctions lists in order to prevent sanctioned individuals from opening a Player Account. The Company has tools in place to conduct the necessary screenings. With the identification of an individual on any of the sanction lists, the Company will proceed to reject the account opening or in case of a later listing, proceed to freeze the account. The case will then be escalated to Compliance for further investigation and reporting to the FIU.

- Residents from Restricted Jurisdictions

The Company uses geo-blocking measures in place to prevent residents of Restricted Jurisdictions from accessing the Website.

- Politically Exposed Persons (PEP)

The Company shall implement appropriate risk management systems to determine whether a customer is a Politically Exposed Person (PEP). Upon the identification of a PEP, the Company immediately proceeds to perform Enhanced Due Diligence. Depending on the outcome the application will be rejected or escalated to Compliance for further investigation and possible reporting to the FIU.

A player profile is created based on the information collected to draw up the CRA. The proper level of CDD is then applied and is to be reviewed at a later stage of the business relationship which may result in the adjustment of the risk rating of the player

Simultaneous to the opening of the account, the Company will conduct a PEP and sanctions screening.

Situations involving PEP require the application of EDD measures, independently of the outcome of the risk assessment. This entails having to determine whether a customer 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 XCG 4.000 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 it would have to terminate the business relationship with the said Account Holder.

3.3 The Monitoring of Account Holder activities

The Company takes reasonable steps to prevent activities of money laundering and terrorism financing and constantly monitors all Player activities including financial habits and behavior in order to mitigate industry related risks such as money laundering, terrorism financing and other criminal activities such as fraud.

3.3.1 Unusual activities

The Company has systems in place to monitor the activities on the Player Accounts for the presence of any unusual or suspicious. These activities include but are not limited to:

Duplicate or multiple Player Accounts

Any Player Accounts containing the same personal information, IP address or bank account is considered to be a duplicate account. It is not permitted for an Account Holder to have duplicate Player Accounts or manage more than one (1) Player Account when using the Services on the Website including but not limited to the web-based version. If the Company becomes aware, suspects or believes that this might be the case it reserves the right to immediately terminate any and all Player Accounts held and the Player Account balances either deemed as forfeited by the Account Holder in which event the deposit will be subject to further investigation by the Company. Any winnings arising from such behavior will be forfeited.

Collusion

Upon the suspicion of the multiple registration by Account holders acting in collusion or as a syndicate, the setup of fictitious Player Accounts or the use of front men, the Company reserves the right to change or terminate any bonus offer, cancel any winnings and close Player Accounts.

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 amount deposited will be subject to further investigation.

3.3.2 Deposits and Withdrawals

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.

Deposits

An Account Holder 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.

Withdrawals

An Account Holder can only make a withdrawal request once the initial deposit amount is fully used, and specific bonus terms of a bonus must be satisfied before requesting its withdrawal. No withdrawal will be processed, and funds cannot be withdrawn from the Player's Player Account until:

- i. the required verification checks have been satisfactorily completed (amongst which the Identification checks and screenings against sanction lists);
- ii. payments have been confirmed; and
- iii. the Player has complied with any other withdrawal conditions, specific rules and promotional terms relating to the Player's use of the Website and/or affecting his/her Player Account (for example, any applicable bonus terms), and (iv) wagering activity has been conducted by the Player in a minimum amount to be further determined by the Compliance function.

If following a screening the Company becomes aware that a Player appears on a Sanction list as a designated person or entity, the Company will immediately proceed to freeze the account without delay and without prior notice. The CO will proceed to file a report with the FIU. Following an established match, the player relation will be terminated and the funds will remain frozen.

Withdrawal requests can only be addressed to the Account Holder registered on the Player Account and only to the account from which deposits were made. The information provided on the withdrawal form must be identical to the personal data held by the Company. Withdrawal requests made to other parties will not be taken into consideration.

3.3.3 Transactions using Cryptocurrency

In those cases where Player requests payment in Crypto, the following will be applicable.

Crypto 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 will further conduct the following procedure:

- Collect and verify proof of identity and proof of address as described above in the 'Customer 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 maintain and provide proof of balance (as may be acceptable by the Regulator) to ensure Player's funds have been deposited. The Company will make this available to the Regulator on demand;
- Provide proof of Solvency as per the requirements of the Regulator on a periodic basis (weekly, monthly or as deem fit by the Regulator), 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 highlight 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 might need to be updated accordingly.

3.3.4 Ongoing monitoring

The Company shall conduct ongoing monitoring of the business relationships to ensure that transactions are consistent with the Company's knowledge of the customer; their risk profile, and where necessary the source of funds. The Company reserves the right to carry out a review of the Player Account at any time to confirm the identity, age and/or registration details provided by the Account Holder, in order to ensure that the Customer's use of the services complies with the Terms and Conditions and all 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 information provided may be used, recorded and disclosed and that the data may be recorded by the Company or engaged third party.

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.

3.4 Reporting of unusual transactions

In accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Company is required, as online gaming provider, to detect and report either intended or completed unusual transactions. Following the monitoring of the player activities as described in section 3.3 above, the Company is able to detect whether a transaction or series of transactions is unusual compared to the expected activities of the player. The

NORUT has established objective and subjective indicators through which an operator must determine whether a player's transaction qualifies as an unusual transaction that should be reported to the FIU.

Objective indicators

If a player transaction or activity coincides with the circumstance described in the indicator, this must be deemed unusual and mandatorily reported to the FIU as an unusual transaction.

The objective indicators are:

- A. A transaction that is reported to the police or the judicial authorities in connection with money laundering or the financing of terrorism.
- B. An intended transaction by or for the benefit of a natural person, legal person, group or entity, that is mentioned on a list that has been drawn up pursuant to the Sanctions National Ordinance.
- C. A transaction of the value of XCG 5,000 or more (or its equivalent in foreign currency), regardless of the method of payment, be it cash or other form of payment, electronically or by another non-physical way; including amongst others:
 - 1. A transfer from the bank account of the operator to a local or international bank account at the request of the player;
 - 2. Taking funds in deposit or releasing funds held in deposit at the request of a player;
 - 3. Selling tokens (which includes chips and credits) to a player; and
 - 4. Pay-out of prize money.

Transactions may be a single transaction, a series of transactions combination or pattern of transactions involving a total amount of monetary equivalent of XCG 5,000 (or its equivalent in foreign currency) or more and is considered per gaming day.

Subjective indicators

Any transaction that gives reason to assume it could be related to money laundering or to the financing of terrorism is categorized as a subjective indicator.

A transaction gives reason to assume it could be related to ML or TF where there is any grounds for suspicion (or knowledge) of money laundering, terrorist financing, or proliferation financing.

An unusual activity may arise from, but is not limited to, findings identified through:

- Customer risk classification and monitoring activities described in section 'Client Risk Classification';
- Ongoing transaction and behavioral monitoring described in 'Monitoring of Account Holder Activities';
- Identification of unusual activities as outlined in 'Unusual Activities';
- Enhanced Due Diligence measures applied under Section 'Enhanced Due Diligence'.

Unusual transactions or any intention thereto must be reported to the FIU without delay.

Under no circumstances shall the customer be informed of the report (tipping-off prohibition).

The following procedures for internal and external reporting are followed.

3.4.1 Internal Unusual Activity Reporting

All Employees and any persons acting on behalf of the Company, as defined under Section 1.3 (Scope), have a duty to remain vigilant and to promptly report any circumstance which is deemed unusual if one or more of the mentioned indicators apply.

Where an Employee identifies a transaction to be in line with an objective- or a subjective indicator, the Employee must immediately report the transaction internally to the Compliance Officer (CO), as defined in section 'The Compliance Officer', regardless of the transaction amount and without delay.

Internal reports shall:

- Be submitted as soon as practicable after the circumstance arises;
- Contain all relevant information known to the reporting Employee, including transaction details, customer information collected under section 'Know Your Customer Procedure', and monitoring findings;
- Be documented in a confidential manner, using internal reporting tools or forms as determined by the CO.

3.4.2 External Unusual Activity Reporting

Upon receipt of an internal unusual activity report submitted in accordance with Section 3.4.1, the CO shall determine whether the reported activity is categorized as an objective- or subjective indicator and should further review all relevant information, including:

- Customer identification and verification records collected pursuant to section Know Your Customer Procedure;

- Transaction data and behavioral indicators identified through monitoring activities under section Monitoring of Account Holder Activities;
- Risk factors identified through the Customer Risk Assessment outlined in the relevant section

Where the CO establishes a transaction to be falling under the scope of an objective indicator or further determines a transaction to be related to ML, TF or PF, the CO shall proceed to file a report with the FIU in accordance with the NORUT, as referenced in Section 2.1 (National Regulations).

External reporting shall:

- Be submitted without undue delay following the determination of suspicion;
- Be made exclusively by the CO or a formally designated alternate in line with responsibilities set out in Section 4 Money Laundering Reporting Officer;
- Include all relevant and available information required by the FIU.

The CO shall ensure that:

- All submitted reports and supporting documentation are retained in accordance with section Recordkeeping;
- Decisions not to report are sufficiently supported, properly documented and retained, consistent with the documentation standards referenced in section Reporting of Unusual Transactions;
- Ongoing monitoring under section Ongoing Monitoring continues where appropriate, unless otherwise instructed by competent authorities.
- Further review is conducted. Any unusual transactions or circumstances for which the Company has not received sufficient explanation may give rise to its report to the Curaçao FIU.

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.

Further review is conducted. Any unusual transactions or circumstances for which the Company has not received sufficient explanation may give rise to its report to the Curaçao FIU.

3.5 Recordkeeping

The Company maintains a record of all relevant documentation such as Customer identification information, transaction records, internal and external reports, and information

on the compliance training 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. The Compliance Function (CF)

The Company has designated an Compliance Officer (CO) that acts independent from games operations and is responsible for the detection and deterrence of ML and TF. The position of the CO is crucial for ensuring that our operations adhere to the regulatory requirements and standards pertinent to the gambling industry.

The CO is in charge of the following amongst others:

- Monitoring and adherence to legal and regulatory standards;
- Reporting to the relevant AML/CTF authorities;
- Designing, implementing and make the necessary changes to the AML program;
- Ensuring compliance with Curaçao laws and regulations regarding money laundering and terrorist financing;
- Reviewing adherence to the policies and procedures maintained by the Company;
- Analyzing transactions and identifying those subject to reporting under the Ministerial Decree on Indicators for Unusual Transactions;
- Reviewing internally reported unusual transactions for completeness and accuracy;
- Design an internal procedure about when reporting of unusual transactions will lead to blocking/ freezing of user accounts;
- Conducting further investigations into unusual transactions if necessary;
- Preparing external reports on unusual transactions;
- Maintaining records of both internally and externally reported unusual transactions;
- Preparing periodic reports on the efforts against money laundering, terrorism financing, an proliferation financing conducted by the Company
- Organizing staff training sessions on compliance-related issues.

The CO is further assisted by designated personnel.

5. Training

In order 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 CO 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 in accordance with the role of the employee within the organization;
- 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.

6. Staff Due Diligence

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. This information is used to initiate pre-employment checks and screening with the support of third-party screening providers.

7. 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 an Employee or group of Employees (not being the CO and not under the direct reporting line of the CO), so long as the reviewer is sufficiently independent and qualified to ensure that the findings and conclusions are reliable.

The review will be focused on the following items at the minimum:

- Evaluation of the AML manual;
- Customer's file review;
- Transaction testing;
- Assessment of training adequacy;
- Assessment with compliance with applicable laws and regulations
- Evaluation of the system's ability to identify unusual activity;
- Sampling of unusual transactions followed by a review of compliance with the internal and external policies and reporting requirements; and
- Assessment of the adequacy of the record retention system.

The findings and conclusions will be documented, with any deficiencies reported to management, with a request to take corrective actions such as amendment or enhancement of controls and procedures, by a certain deadline.

8. Examination by the Curaçao Gaming Authority (CGA)

The Regulator may, in connection with its supervisory role, request any information or documentation in preparation for, or during an examination as well as at any time during the year, as necessary to supervise compliance with the provisions of or pursuant to the applicable legislation. The Company shall cooperate with the Regulator and make available any documentation or information reasonably required for the proper performance of their supervisory duties.

Contact Information

For any questions regarding this policy, please contact:

eMoore N.V.
Legalcompliance Department
Groot Kwartierweg 10, Livestrong Building
Willemstad, Curaçao
Telephone: +599 9 7471401
Email: legalcompliance@the-emgroup.com