

**POLICIES AND PROCEDURES TO DETECT AND PREVENT MONEY
LAUNDERING, TERRORIST FINANCING AND CORRUPTION**

BETTINGSPOON B.V.

(the “Company”)

June 2026

Signature: *C. Drommond*
Name: C. Drommond, Proxyholder of eMoore N.V.
Date: June 4, 2026]

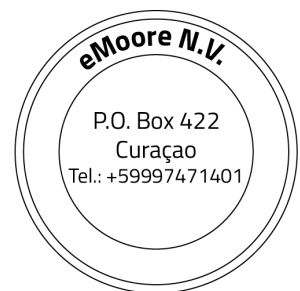


TABLE OF CONTENTS

VERSION HISTORY	4
AREAS COVERED BY THIS MANUAL	5
DISCLAIMER	5
INTRODUCTION	6
THE PURPOSE AND IMPORTANCE OF THE COMPLIANCE FUNCTION	9
REGULATORY FRAMEWORK APPLICABLE TO THE COMPANY	10
RISK MANAGEMENT	12
Risk assessment	13
Business risk assessment (BRA)	13
Customer Risk Assessment (CRA).....	18
CLIENT IDENTIFICATION POLICIES AND PROCEDURES	23
Client Risk Classification	24
Know Your Customer Procedure.....	24
Customer Due Diligence	25
Simplified Due Diligence	25
Standard Due Diligence.....	25
Enhanced Due Diligence	27
Politically Exposed Persons (PEPs).....	29
Corruption and Bribery Prevention Procedures	31
COMPLIANCE PROCEDURES: CHECKS AND BALANCES	33
Ongoing Monitoring Procedures and Internal Controls	33
The Monitoring of client activities	33
Continuous transaction due diligence.....	37
REPORTING POLICIES AND PROCEDURES	38
The Compliance Function (CF).....	38
Reporting of unusual transactions.....	39

Objective indicators	39
Subjective indicators	40
Internal Unusual Activity Reporting	40
External Unusual Activity Reporting	41
Tipping Off.....	41
RECORD KEEPING POLICIES AND PROCEDURES	42
ANTI-MONEY LAUNDERING TRAINING POLICIES	42
STAFF DUE DILIGENCE	43
PERIODICAL REVIEW OF AML/CFT POLICIES.....	43
Examination by the Curaçao Gaming Authority (CGA).....	44
Contact Information	44

VERSION HISTORY

Version #	Effective Date	Approving Official	Responsible Office	Next Review Date	Comments
1.0	July, 2022	Downtown E-commerce Company B.V.	Compliance function	Undefined	-
2.0	May 30, 2026	eMoore N.V.	Compliance function	May 30, 2027	-

AREAS COVERED BY THIS MANUAL

The general areas covered by this Manual include the following:

- the purpose and importance of the compliance function;
- Risk Management including Business Risk Assessment and Customer risk assessment
- Client identification policies and procedures;
- the procedures that will be used to test compliance and how breaches in compliance will be reported and rectified; and
- Record keeping.

DISCLAIMER

This Policies and Procedures Manual (**Manual**) provides guidelines to the Company to meet its obligations under the National Ordinance on identification when rendering services (Landsverordening identificatie bij dienstverlening (LID), PB 2017, no. 92), the National Ordinance on the reporting of unusual transactions (Landsverordening melding ongebruikelijke transacties (LMOT), PB 2017, no. 99), and the National Ordinance on Games of Chance (Landsverordening op de Kansspelen (LOK), PB 2027, no. 157).

This Manual is intended to assist the Company with meeting the regulatory obligations to which it is subject in Curaçao as at the date of this Manual.

INTRODUCTION

Money Laundering (ML), Terrorism Financing (TF) and Proliferation of weapons of mass destruction or Proliferation Financing (PF) pose significant and evolving risks to national and international financial systems. In line with the Financial action Task Force (FATF) Recommendations, vulnerable sectors are required to implement effective, risk-based measures to prevent their misuse for these purposes primarily, as well as for any other illicit activities. This Manual establishes the necessary procedures to be followed to prevent and mitigate the risks of money laundering, terrorist financing and proliferation of weapons of mass destruction primarily. The Company is committed to full compliance with all applicable legal and regulatory obligations and to the effective management of ML/TF/PF risks through a risk-based approach. Special attention is also paid to mitigating the risk of corruption.

Money laundering is characterized by an attempt to conceal the illegal source of the funds and transform them into legitimate funds through complex transactions typically orchestrated through numerous entities. Money laundering is generally motivated by illegal or criminal activity, once laundered; funds derived from illegal means can more easily be used for other purposes.

Deception is the heart of money laundering and by its very nature it is a hidden activity, the general consensus amongst worldwide regulatory bodies is that there are three stages of money laundering:

- Placement: placing cash proceeds/assets of criminal conduct into the banking system;
- Layering: creating complex layers of transactions to conceal the origin of the funds; and
- Integration: proceeds now appear legitimate and are “integrated” into the financial system.

Curaçao legislation criminalizes terrorism and terrorist financing, following UN conventions and international standards. Dealing with property intended to be used for terrorist purposes, or being involved in any arrangement in support of terrorism, are serious criminal offences. The financing of terrorism is characterized by the solicitation and collection of funds or assets which are intended to be put to a terrorist purpose. Whilst similar to money laundering, terrorist financing can be distinguished by the fact that the funds involved are not necessarily “dirty”. Funds of a perfectly legitimate source become criminal property by virtue of the use to which they will be put.

Proliferation of Weapons of Mass Destruction 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 identified by relevant United Nations Security Council Resolutions (UNSCRs). Therefore, the 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

Bribery is a criminal offence and corrupt acts expose the Company and its employees not only to reputational risk but to the risk of prosecution, fines and imprisonment. Bribery is often characterized by the offering or receiving of payment or some benefit in exchange for the exercise of influence, particularly with respect to the awarding of contracts. Domestic legislation in Curaçao makes bribery and corruption a serious offence. The legislation of other jurisdictions, particularly England and the European Union, has extra-territorial reach. As such, a “zero-tolerance” approach is taken to acts of bribery or corruption and care must be taken to comply with not only the letter but the spirit of the law.

Accordingly, the Company has established anti-money laundering, counter-terrorist financing and counter-proliferation financing policies and controls that are consistent with the highest international standards, including those issued by the FATF.

The objective of this Policy is to outline the AML/CFT strategy of the Company in order to:

- a) ensure that the Company can manage its compliance risk, i.e. the risk of legal and regulatory sanctions, material financial loss or reputational damage that the Company may suffer as a result of failing to comply with its regulatory and its anti-money laundering, terrorism and corruption obligations
- b) ensure that the Company does not enter into, or maintain, relationships with individuals or entities whose conduct raises suspicions of involvement in money laundering (ML) and/or terrorist financing (TF);
- c) terminate any existing relationships where the client’s conduct provides reasonable grounds for suspicion of involvement in illegal activities. Such termination shall only occur after the relevant suspicion has been reported and shall be carried out in coordination with the appropriate authorities and in compliance with applicable regulations;
- d) adhere to the Company’s anti-money laundering (AML), counter-terrorist financing (CFT), and counter-proliferation financing (CPF) obligations in line with both national and international regulatory requirements; and
- e) maintain accurate and comprehensive records to facilitate effective supervisory and regulatory oversight.

This policy applies to all employees and form an integral part of the Company's governance and compliance framework. It 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

THE PURPOSE AND IMPORTANCE OF THE COMPLIANCE FUNCTION

The overall objective of the compliance function is to ensure that the Company complies with its regulatory obligations under the anti-money laundering, terrorism and corruption legislation applicable in Curaçao and any other jurisdiction in which the Company operates. The compliance function is also concerned with the Company's ability to demonstrate the existence and effectiveness of our systems and controls.

Compliance is the responsibility of the Company and, within the Company, ultimate responsibility for compliance lies with the Company's Board of Directors.

REGULATORY FRAMEWORK APPLICABLE TO THE COMPANY

The infrastructure for anti-money laundering and combating the financing of terrorism (AML/CFT) on Curaçao finds its legal basis in the National Ordinance on identification when rendering services (LID) and the National Ordinance on the reporting of unusual transactions (LMOT). These ordinances determine that all service providers offering the opportunity to participate in online gaming, fall within the regulatory scope.

The money laundering provisions apply to “criminal conduct” which includes the laundering of an offender’s own proceeds of crime as well as assisting in the laundering of someone else’s proceeds. Criminal offences fall into the following principal categories, and a person commits an offence if he:

- conceals, disguises, converts or transfers criminal property or removes criminal property from Curaçao;
- enters into or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person;
- acquires, uses or has possession of criminal property;
- fails to disclose to a Compliance function or the Financial Intelligence Unit (**FIU**) suspicion or knowledge of another person engaging in a prohibited act. Disclosure of suspicion to the FIU is a defense, however, failure to disclose may be subject to a “negligence test” whereby the Courts may rule that a person had “reasonable grounds” for knowing or suspecting criminal conduct even if they did not actually know or suspect; and
- makes a disclosure (other than to the FIU) which is likely to prejudice an investigation being or about to be conducted by the FIU (tipping off).

The Regulations also require that relevant businesses have in place anti-money laundering policies, procedures and practices to facilitate the relevant business’s ability to comply with the anti-money laundering regime of Curaçao. Specifically, the Regulations require that relevant businesses should not form business relationships or carry out one-off transactions with or for another person unless they:

- maintain procedures, which establish and verify the identity of clients;
- adopt a risk-based approach to monitor financial activities and maintain adequate systems to identify risk in relation to persons, countries and activities;
- maintain procedures to screen employees to ensure high standards when hiring;
- maintain record-keeping procedures;

- establish internal reporting procedures;
- adopt appropriate internal controls and ongoing monitoring procedures;
- maintain and monitor record keeping in respect of client identification, accounts files and business correspondence in respect of the transactions of such clients;
- provide appropriate AML training in accordance with the Regulations (where applicable); and
- Designate a Compliance Officer.

Further 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 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);
- d) 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
- e) 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.
- f) National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- g) Sanctions National Ordinance (N.G. 2014, no. 55)
- h) Kingdom Sanction Act (N.G. 2016, no. 54);
- i) 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 regulatory instruments issued and upheld by the Curaçao Gaming Authority (CGA) as the online gaming regulator in Curaçao, serve to ensure fair, responsible, and corruption-free gaming, strengthening the industry overall

On an international level, the Financial Action Task Force (FATF) plays an important role in the combating of ML, TF and PF. The FATF together with its associate members and regional branches, 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. As a

member of the FATF¹ and of the regional branch, the Caribbean Financial Action Task Force (www.cfatf-gafic.org), Curaçao is meeting international standards by regularly implementing these standards in its national legislation

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.

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
- vi. weaknesses; and
- vii. Review and update risk assessments periodically or upon material changes.

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.

¹ www.fatf-gafi.org

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.

Business risk assessment (BRA)

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 corresponding 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 behavior 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 behavior.

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 the 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 gambling	Market	3	5	15
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	clients 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 table presents the mitigation strategy to be implemented, the effectivity rate, the activities to reduce residual risk, and 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	15	9	6	Medium

	response planning				
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.

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 present 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.

The Company maintains a list of restricted jurisdictions, including those prohibited under the licensing conditions set by the Curaçao Gaming Authority (CGA), as well as jurisdictions restricted by decision of the Company's Managing Director, where applicable. This list also includes countries designated on the FATF blacklist and those subject to financial sanctions imposed by the European Union, the United Nations, and/or the U.S. Office of Foreign Assets Control (OFAC).

At present the current jurisdictions on the list are:

United States of America and all its dependencies territories and its minor outlying islands, United Kingdom, Spain, France, Curaçao, Netherlands, 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.

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 behavior	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 behavior	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

CLIENT IDENTIFICATION POLICIES AND PROCEDURES

The Company has an obligation to determine that money-laundering activities are not being conducted. The first line of defense against any money laundering activity is to **KNOW YOUR CLIENT**. In effect, this means that standard client identification must be collected on every client. The Company will apply a “Risk-

Based” analysis as required under the Regulations to determine the level of client due diligence measures to be applied to the client.

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 client.

The Company maintains the following risk classification:

- Low risk
- Medium risk
- High risk

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

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, a client 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.

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 customers. No establishment of the identifying of beneficial owner is in place. At all times identification can be requested establishing the identity of the client.

The Company applies to 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 client activity on the platform, if required

Simplified Due Diligence

Simplified Due Diligence is conducted at account opening, in low-risk scenarios. The Company will request the information as indicated in the section “Know Your Customer Procedure” 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.

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 client 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 the 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 client account without the refund of the deposited amount.

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 client 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:

- i. verifying the disclosed details against certain (public or private) databases (e.g. sanction lists);
- ii. ordering a credit report;
- iii. bank statement showing the initial deposit;
- iv. request to provide information/ documentation showing source of funds/wealth.

The Company reserves the right to restrict the client 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 client account and suspension of any of the outstanding balance

The Residual risk level further determines the monitoring frequency of the relevant client and its activities on the platform.

Type of Client	Monitoring frequency
Clients 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 Clients, High-Rollers, PEPs with lower relative risk and active Clients from high-risk jurisdictions	Weekly (or upon a material change)
Medium Risk Clients	Every six months (or upon a material change)
Low Risk Clients	Annually (or upon a material change)

High-Risk Countries

Certain countries are associated with crimes such as drug trafficking, fraud, corruption etc. and consequently pose a higher risk to the Company. The Company should conduct enhanced due diligence on entities/individuals based in high-risk countries and caution against the acceptance of certified documentation from these countries. High Risk countries are listed at the FINCEN, OFAC and Transparency International websites.

Restricted Persons

The Company has determined the following customer categories to represent a high and or higher than average risk of ML/TF/PF. 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.

The Company will not enter into any business relationship or financial transaction with a person that:

- is younger than 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;
- is not a natural person. 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.

- is on any trade or economic sanctions lists, such as, but not limited to, the UN Security Council Sanctions list, designated as a “Specially Designated National” by OFAC (Office of Foreign Assets Control of the U.S. Treasury Department) or placed on the U.S. Commerce Department’s “Denied Persons List”. The Company screens all applicants against international sanctions lists in order to prevent sanctioned individuals from opening a client 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.
- is a Government Official or Politically Exposed Person within the meaning of the FATF’s 40 Recommendations;
- is from or in jurisdictions that does not meet international AML–CTF standards as set out by the FATF as high-risk, non-cooperative, and strategically deficient jurisdictions, including but not limited to the Democratic People’s Republic of Korea (North Korea), Ethiopia, Iran, Iraq, Sri Lanka, Syria, Trinidad & Tobago, Tunisia, or Yemen.
- presents a risk of any exposure to penalties, sanctions, or other liabilities under AML Laws, CTF Laws, Anti-Corruption Laws, Economic Sanctions Laws, or tax Laws that may apply;
- fails to provide his/her full name as well as further personal information at registration. It is impossible to open an account without providing personal information. An individual can only play on their own behalf, not for other individuals nor for legal persons.
- fails to meet any user due diligence standards, requests, or requirements of the Company, or otherwise appears to be of high risk, including but not limited to any of the foregoing factors;
- it is resident in a restricted jurisdiction, as decided by the Company from time to time.

Politically Exposed Persons (PEPs)

The Company should also conduct enhanced due diligence and apply a higher degree of vigilance when dealing with PEPs. An explanation as to what constitutes a PEP is stated below:

- a person who is or has been entrusted with prominent public functions by a foreign country, for example a Head of State or of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and important political party official;

- a person who is or has been entrusted domestically with prominent public functions, for example a Head of State or of government, senior politician, senior government, judicial or military official, senior executives of a state-owned corporation and important political party official; and
- a person who is or has been entrusted with a prominent function by an international organization like a member of senior management, such as a director, deputy director and a member of the board or equivalent functions. The risks occur when these persons abuse their public powers and basically filter their ill-gotten funds to offshore jurisdictions.

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.

The Regulations impose a requirement for regulated entities such as the Company to be vigilant in relation to PEPs and have risk management policies in place to:

- determine whether the client is a PEP, a family member (includes the spouse, parent, sibling, or child of a PEP) or close associate (includes any natural person who is known to hold ownership or control of a legal instrument or person jointly with a PEP, who maintains some other kind of close business or personal relationship with a PEP, or who holds the ownership or control of a legal instrument or person which is known to have established to the benefit of a PEP);
- obtain senior management approval for establishing business with a PEP, a family member or a close associate;
- take measures to obtain source of funds information; and
- conduct enhanced monitoring of the relationship.

Should a client who had not been identified as a PEP at on-boarding stage result to have become one, an employee is required to carry out or implement these measures described within the thirty (30) day window, failing which it would have to terminate the business relationship with the said client.

The degree of scrutiny that the Company will apply will depend on various risk factors, including, but not limited to:

- proof that the client's source of funds or wealth do not emanate from criminal activity;
- whether the home jurisdiction of the PEP is one in which current or former political figures have been implicated in corruption; and
- the length of time that a former political figure has been in office.

Upon the identification of a PEP, the Company immediately proceeds to perform Enhanced Due Diligence. Depending on the outcome or if due diligence cannot be performed adequately, the Company should consider not opening the account, suspending the transaction activity, filing a report with the MLRO or closing the account.

Corruption and Bribery Prevention Procedures

The due diligence procedures outlined above are vital not only in relation to anti-money-laundering and terrorist financing concerns, but to anti-bribery and corruption as well. In the context of bribery and corruption legislation, it is essential to know your business partners. The robust take-on procedures described above for potential clients (particularly the PEP procedures) operate to identify situations of high risk for bribery and corruption at the initial stages of the relationship. However, it is possible that the Company or its staff may become indirectly involved with bribery and corruption later in the relationship, or by way of association with third parties. Therefore, consideration should be given as to whether it is necessary to carry out due diligence on certain associates, agents, contractors, facilitators and others with whom the Company has a business relationship where there may be a risk of bribery and corruption.

If during the course of their duties a member of staff becomes suspicious of any client, business partner or staff member being involved in any way in bribery or corruption, they should immediately inform the MLRO. The reporting process in place to report a suspicion of money-laundering should be used. The MLRO will determine whether further action, including reporting to the authorities, is appropriate and should document the decision and keep a log of any such reports.

Care must be taken to ensure that the Company's legitimate business promotion initiatives do not fall afoul of the bribery and corruption legislation or this policy. Such initiatives include:

- The giving of gifts or tokens of appreciation to clients or business partners;
- Client entertainment and hospitality;
- Invitations to events, functions, or other social gatherings in connection with matters related to our business.

These kinds of activities are recognized as an established and important part of doing business, provided they fall within reasonable bounds of value and occurrence. A variety of cultural factors such as customs, currency, and expectations may influence the level of acceptability.

A reasonable level of discretion is permitted with respect to such activities. Giving gifts to clients must be reasonable and proportionate. Unduly lavish gifts are prohibited as they could give rise to the inference of impropriety. Care is to be taken in relation to the timing of gifts as there must be no inference that the gift relates to the recipient being involved in a pending decision affecting the Company. (For avoidance of doubt, a gift also includes the provision of free services.) It is the policy of the Company that any proposed gift of a value of \$125 or more must be approved by the MLRO in advance.

Occasionally staff members will be offered a gift from a client or other business partner to show gratitude for the work that they have done. No gift and/or favor of whatever kind may be accepted from any client or supplier of the Company that would in any way influence or reasonably be considered to influence the staff member to act inappropriately. In the event of a gift, benefit or inducement of any kind being offered to a member of staff by a client or business partner with a value likely to be more than US\$125, the details must be reported to the Compliance function.

If a member of staff feels uncertain at any time regarding acceptability of gifts, entertainment or hospitality, please consult the Compliance function.

COMPLIANCE PROCEDURES: CHECKS AND BALANCES

Compliance, Risk Management and the overall ethical culture of the Company are the direct responsibility of the Board of Directors of the Company.

The Company adheres to proper procedures. Senior management must practice high standards of ethics, compliance and proper risk management themselves and within their respective area of responsibility.

Ongoing Monitoring Procedures and Internal Controls

The Monitoring of client activities

The Company takes reasonable steps to prevent activities of money laundering and terrorism financing and constantly monitors all client 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.

Unusual activities

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

- Duplicate or multiple client accounts

Any client accounts containing the same personal information, IP address or bank account is considered to be a duplicate account. It is not permitted for a client to have duplicate client accounts or manage more than one (1) client account when using the services on the website operated by the Company 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 client accounts held and the client account balances either deemed as forfeited by the client 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 client accounts or the use of front men, the Company reserves the right to change or terminate any bonus offer, cancel any winnings and close client accounts.

- Identity fraud

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

Deposits and Withdrawals

All financial transactions must match the name of the credit card or other payment accounts through which the client 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 client account subject to further investigation.

- Deposits

A client 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 to data held by the Company.

A client may deposit money in his client account only in order to play on the website operated by the Company 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 clients.

- Withdrawals

A client 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 client's 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 client has complied with any other withdrawal conditions, specific rules and promotional terms relating to the client's use of the website operated by the Company, and/or affecting his/her client account (for example, any applicable bonus terms), and (iv) wagering activity has been conducted by the client in a minimum amount to be further determined by the Compliance function.

If following a screening the Company becomes aware that a client 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 client registered on the client 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.

Transactions using Cryptocurrency

In those cases where client 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 client 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 client 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 client (IP and computer);
- The Company will maintain and provide proof of balance (as may be acceptable by the Regulator) to ensure client'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 client may deposit money into the client account only in order to play and to use the services. Likewise, the client may only withdraw winnings and not the funds deposited into the client account. clients 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 clients.

Notification of new payment methods will be made on the homepage of the Website and sent by e-mail to the client as they are added. For each new depositing method, this Manual and the terms and conditions on the website operated by the Company might need to be updated accordingly.

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 client, in order to ensure that the Customer's use of the services complies with the terms and conditions of the Company 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 by 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 client may be restricted from withdrawing funds from the client account and/ or prevented from accessing certain services offered on the website operated by the Company.

The Company will monitor account activity with special attention, and to the extent possible, the background and purpose of any more complex or large transactions and any transactions which are particularly likely, by their nature, to be related to money laundering or the funding of terrorism.

Monitoring will be conducted through the following methods: Transactions will be automatically monitored and reviewed daily for all transactions above EUR 1000 along with all the details of the users making those transactions. Documents may be required at the determination of the CO.

The CO will be responsible for this monitoring, will review any activity that the monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the relevant authorities.

Parameters that signal possible money laundering or terrorist financing include, but are not limited to:

- Wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent reason.
- Many small, incoming wire transfers or deposits made using checks and money orders.

Wire activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent specific purpose.

Continuous transaction due diligence

When an employee of the Company detects any activity that may be suspicious, he or she will notify the CO who will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or filing a report.

The Company will not accept cash or non-electronic payments from clients. Funds may be received from clients only by any of the following methods: credit cards, debit cards, electronic transfer, wire transfer cheques and any other method approved by the Company or respective regulators.

The Company will only transfer payments of winnings or refunds back to the same route from where the funds originated, where possible.

To the extent the Company utilizes a third party to process and record payments to and from client and accounts, the Company will use best efforts to ensure the services provider has transaction monitoring systems in place which will allow for screening of the transactions pursuant to these provisions and in

accordance with the applicable legislation. The CO shall be responsible to review the relevant service agreement with the service provider to ensure the adequacy of the agreement.

Records relating to the financial transactions shall be maintained in accordance with the data protection and retention requirements in the applicable jurisdiction of Curaçao.

REPORTING POLICIES AND PROCEDURES

The Company is committed to deterring money laundering and any activity that facilitates money laundering or the funding of terrorist activities. The dedication of the Company is reflected in its desire to comply with all laws and regulations designed to combat money laundering activity.

The Compliance Function (CF)

The Company has designated a 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 Compliance function consists of the Compliance Officer (CO), who is further assisted by designated personnel to ensure the effective execution of compliance duties..

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 client 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.

Internal Unusual Activity Reporting

All employees of the Company are required to be familiar with the anti-money laundering procedures and immediately report to the Compliance function the occurrence of any suspicious activity. All Employees and any persons acting on behalf of the Company, 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 function, 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.

In the event that an employee receives any enquiry from a law enforcement agency, that inquiry shall immediately be referred to the Compliance function.

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 client 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 Compliance function 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.

TIPPING OFF

Suspicious activity reports and all supporting documentation are confidential. Tipping off is an actual offence under the legislation and carries with it a monetary fine and jail term. Employees are prohibited from disclosing to anyone, including persons involved in the transaction, information in connection with a

filing of a suspicious activity report. Violation of this policy will result in disciplinary action and termination of employment.

RECORD KEEPING POLICIES AND PROCEDURES

The Company retains client records, including but not limited to, client identification, account opening information, transactional records, internal and external reports, information on the compliance training, relevant account files and business correspondence, for a period of five years following the closing of the account or termination of the business relationship on a separate database.

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.

ANTI-MONEY LAUNDERING TRAINING POLICIES

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.

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.

PERIODICAL REVIEW OF AML/CFT POLICIES

The AML/CFT policies of the Company are subject to a yearly review, comprising 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.

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 informational 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