

Anti Money Laundry Compliance Program

(Including Business Risk Assessment & Customer risk Assessment)

LEGACY EIGHT CURAÇAO N.V.
Groot Kwartierweg 10, Willemstad, Curaçao

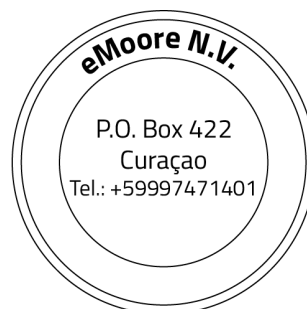
Version control

Policy	Approval date	Approver
Anti money laundering Compliance Program 1.1	10 April	Iván Piña

C. Drommond

eMoore N.V.
Managing Director
By: Cornelia F. Drommond-Oonincx
Proxy holder eMoore N.V.

Date: **14/05/2025**



INDEX

1.	DEFINITIONS AND ABBREVIATIONS	5
2.	ABOUT LEGACY EIGHT CURAÇAO N.V.....	7
3.	POLICY OVERVIEW	7
3.1	Objectives	8
3.2	Scope	8
3.3	Policy Maintenance and Distribution	8
3.3.1	Approval and Dissemination.....	8
3.3.2	Policy Review and Update	8
4.	COMPLIANCE OFFICER.....	9
4.1	Identification and Contact Details	9
4.2	Reporting Structure and Independence	9
4.3	Duties and Responsibilities	9
5.	REGULATORY FRAMEWORK	10
5.1	National Regulation	10
5.2	International regulations	11
6.	BUSINESS RISK ASSESSMENT	11
6.1	Overview.....	11
6.2	Business Services related risks:.....	12
6.2.1	Business Services risk factors:.....	12
6.2.2	Mitigation and controls:	12
6.2.3	Residual risk:.....	13
6.3	Product related risks:.....	13
6.3.1	Product Risk factors:	14
6.3.2	Controls and implementation / residual risk:	14
6.4	Payment source related risks:	14
6.4.1	Low risk – Negligible Source Risk	14
6.4.2	Medium risk – Managed Source Risk.....	15

6.4.3	High risk- Moderate Source Risk.....	15
6.5	Customer related risks:.....	15
6.5.1	Mitigation and controls	16
6.5.2	Residual risk.....	17
6.6	Geographical Risks.....	17
6.6.1	Geographical Risk factors:	18
6.6.2	Residual risk.....	18
7.	SITE SUBSCRIBERS AND CUSTOMER ACCOUNTS (Website visitors Vs Account Registration)	19
7.1	Site Visitors/Marketing Subscribers:	19
7.2	Registering an account/Account Sign-up:.....	19
8.	CAPTURED DATA.....	19
8.1	Data inputted by the account holder on sign-up:.....	20
8.2	Data gathered silently:	20
8.3	Updates and Changes	20
9.	KNOW YOUR CUSTOMER PROCEDURES - Customer Due Dilligence	21
9.1	Identity Validation and Risk Assessment (Simplified DD)	21
9.2	Customer Due Diligence (CDD)	22
9.3	Enhanced Due Diligence (EDD)	23
9.3.1	Overview.....	23
9.3.2	EDD Triggering Events.....	24
10.	RISK MANAGEMENT STRATEGY	24
10.1	General Principles.....	25
10.2	Phase 1 - Preliminary Screening (registration data assessment, identity validation, transaction activity monitoring, and Source confirmation):.....	26
10.3	PHASE 2 – RECURRING CONDUCT ASSESSMENT (On-Going Monitoring)	28
10.4	PHASE 3 – DESTINATION VALIDATION.....	28
10.4.1	Deposits and Withdrawals.....	29
10.4.1.1	Deposits	29
10.4.1.2	Withdrawals.....	29
11.	TRANSACTIONS USING CRYPTOCURRENCY	30
12.	POLITICALLY EXPOSED PERSONS AND SANCTIONED INDIVIDUALS	30
13.	SUSPICIOUS INCIDENTS (Unusual Transactions).....	31
13.1	Identification	31

13.2	Reporting of Suspicious Incidents to the Compliance Officer	31
13.3	Investigation	32
14.	REPORTING SUSPICIOUS INCIDENTS TO THE AUTHORITIES	32
15.	RECORD-KEEPING	32
16.	EMPLOYEE DILIGENCE	33
16.1	Employee Screening	33
16.2	Personnel Training	33
17.	AUDIT FUNCTION	34
18.	OTHER COMMENTS ON HANDLING PERSONAL DATA OF CUSTOMERS	34

1. DEFINITIONS AND ABBREVIATIONS

AML	Anti Money Laundering. 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.
Combatting terrorist financing (CFT)	Combating the Financing of Terrorism. 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 focused on combatting the sale, transfer and export of nuclear, chemical or biological weapons and their means of delivery and related materials.
Cash transaction	The deposit and withdraw of fiat money into and out of a Player Account.
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.
Company	Legacy Eight Curaçao N.V., a limited liability company duly organized under Curaçao law registered with the Chamber of Commerce and Industry in Curaçao under number 139031(0).
Employee	Any person working for the Company.
FATF	Financial Action Task Force (www.fatf-gafi.org)
FIU	Financial Intelligence Unit of Curaçao. Pursuant to FATF Recommendation nº. 26, countries must establish a Financial Intelligence Unit (FIU) that serves as a national centre 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.
FMS	Fraud Monitoring System. FMS is an internal risk managing platform which enable us to identify and handle risk scenarios through preconfigured alerts or “rules”. This tool oversees all our customer’s transaction activity and updates made to customer account information, and is configured with rules that makes it possible to identify an account risk level and acting in consequence since the first purchase attempt, and on every subsequent purchase
KYC	Know Your Client, the mandatory process of identifying and verifying the client's identity when opening a Player Account and periodically over time.

License Holder	Legacy Eight Curaçao N.V. a limited liability company duly organized under Curaçao law, registered with the Chamber of Commerce and Industry in Curaçao under number 139031(0) holds a valid Certificate of Operation issued by the Curaçao Gaming Authority.
ML	Money Laundering: 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 and has completed a successful transaction by using the Services offered on the Website and for which a Player Account has been opened.
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 Account is permitted per person, per IP address, per family and per Shared Environment.
PEP	Politically Exposed Persons
Prohibited Jurisdictions	Jurisdictions prohibited under the Curaçao license conditions (Aruba, Belgium, Bonaire, Curacao, France, Netherlands, Saba, Statia, Sint Maarten, USA) as well as jurisdictions restricted by decision of the Company's managing director.
Shared Environment	While environments with shared internet connections (such as households, workplaces, educational institutions, public libraries, or internet cafés) may typically be subject to account limitations, the Company may, at its sole discretion, more than one account within the same environment. Such exceptions will only be granted upon successful verification of the identity and legitimacy of each individual account holder, in accordance with our KYC and AML procedures
Service	The gaming and betting offers provided through the websites operated by the Company to the Account Holder.
Terms and Conditions	The terms and conditions for the use of the Services, as published on the Website.
TF	Terrorist Financing: 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.

2. ABOUT LEGACY EIGHT CURAÇAO N.V.

Legacy Eight Curaçao N.V. is governed by and construed in accordance with the laws of Curaçao. Upon registration and therefore acceptance of the Terms of Service and Privacy Policy as published in our website, customers expressly agree to submit to the jurisdiction of the courts of Curaçao.

3. POLICY OVERVIEW

Money laundering (ML) and the use of legal or illegal monies for the purpose of financing terrorism (FT) and the proliferation of weapons (FP) have become ever growing threats for national and international economies throughout the world, forcing all vulnerable sectors to have measures in place for the prevention of their misuse for these purposes. Individuals involved in ML and/or TF continually attempt to exploit services and products to conceal their unlawful activities and proceeds' true nature. Illicit efforts by such individuals must be recognized and thwarted by all feasible means. AML policies incorporate regulations and laws for limiting financial criminals from concealing funds collected through illicit sources.

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

- the use of criminal funds to fund gambling activities; and
- 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 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.

Legacy Eight Curaçao N.V. (the “Company”) is fully committed to playing its role in identifying and mitigating such organized crime. The Company has therefore incorporated the following Anti-Money Laundering and Terrorist Financing Policy (the “Policy”), at heart with the FATF Recommendations and the latest Regulations of Curaçao, as part of its operational procedures. 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.

The Company takes the requirements imposed by the Policy with the utmost seriousness, and to that end key employees should familiarize themselves with the content of the Policy and communicate any questions directly to the Compliance Officer.

3.1 Objectives

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

- 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;
- 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;
- 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
- comply with the Company's AML, CFT and CPF obligations based on national and international regulations.

3.2 Scope

This Policy applies to all members' personal details, business channels, member transactions, and key personnel across the business.

Failure to comply with the procedures set out in this Policy will lead to disciplinary action being taken up to and including termination of employment.

3.3 Policy Maintenance and Distribution

3.3.1 Approval and Dissemination

This Policy has been reviewed and approved by the Compliance Officer and the Director in March 2025. The Policy is furnished to all relevant staff and is redistributed as updated.

3.3.2 Policy Review and Update

The Compliance Officer is responsible for reporting to the Director, Executive Management team and external institutions as settled on the Curaçao Gaming Board's portal (<https://www.gamingcontrolcuracao.org/regulation/aml>) specifically the Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction and other related regulations of any breaches, suspicious activities, or lack in effectiveness of the Policy and related operational procedures as they may be detected and shall provide recommendations to management as to proposed operational or policy enhancements.

Proposed amendments to the Policy require the review and approval of the Compliance Officer, Executive Management team and the Director all of which must review the contents of this Policy for necessary revisions or updates at least once every twelve (12) months. To ensure that the Company is in full compliance with relevant laws and regulations, the Policy is also revised with the introduction of new payment methods, new customer acquisition channels, new markets, and new games or regulatory changes, and new risk scenarios as they may arise.

4. COMPLIANCE OFFICER

4.1 Identification and Contact Details

The Compliance Officer is as follows:

- Ivan Piña Moreno
- Payment Risk Operations and Compliance Manager
- Rambla Republica de México 6517, Montevideo, Uruguay
- ivan.pina@litermi.com
- Tel: +34 620436805

The Compliance Officer has been identified before all Company employees through dissemination of this Policy, as provided and made available to all staff.

4.2 Reporting Structure and Independence

The Compliance Officer reports directly to the Executive Team in respect of his duties under this policy. Subject to oversight by the Executive Team, the Compliance Officer has the authority to act independently from other functions within the organization to fulfil his below-noted roles and responsibilities.

The Compliance Officer has the full and public support of the Executive Management Team in executing his duties. All Company staff are required to assist the Compliance Officer in fulfilling his duties.

4.3 Duties and Responsibilities

The Compliance Officer is responsible for oversight and management of all compliance related functions within the Company, including the protocols and operational procedures described in this Policy. The Compliance Officer duties include the following:

- I. To design and implement the AML program,
- II. To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing,
- III. To review compliance with the Company's policy and procedures,
- IV. To organize training sessions for the staff on compliance-related issues,
- V. To analyse transactions and verify whether any are subject to reporting to the authorities as unusual transactions,

- VI. keep a list of registered Account Holders;
- VII. To review all internally reported unusual transactions for their completeness and accuracy,
- VIII. To keep records of internally and externally reported unusual transactions,
- IX. To design an internal procedure about when reporting unusual transactions will lead to blocking/freezing of user accounts, taking into account the risk of tipping off the player
- X. To execute close investigation of unusual transactions if necessary,
- XI. To prepare the external report of unusual transactions,
- XII. To make necessary changes to the AML program,
- XIII. To remain informed on the local and international developments on money laundering and terrorist financing, and to make suggestions to management for improvements,
- XIV. To prepare periodic information on the casino's efforts against money laundering and financing of terrorism, and financing of proliferation, and,
- XV. Evaluate the efficacy of the policy and suggest improvements as risks change with time;
- XVI. cooperate with all relevant administrative, enforcement and judicial authorities in their endeavour to prevent and detect criminal activity.

5. REGULATORY FRAMEWORK

5.1 National Regulation

Pursuant to the Code of Criminal Law (Penal Code) (N.G. 2011, no. 48), money laundering is a criminal offence in Curaçao.

Further main national regulations relating to money laundering and terrorist financing are the following:

- The National Ordinance on Money Laundering (P.B. 1993, no. 52);
- 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;
- 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;
- 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);
- 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

- 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.
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- These laws and decrees serve as the basis for the procedures maintained by the financial sector of Curaçao to detect and deter industry related risks for money laundering, the financing of terrorism or other criminal activities.

5.2 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 and the TF and proliferation of weapons of mass destruction.

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.

6. BUSINESS RISK ASSESSMENT

6.1 Overview

The Company operates a lottery betting and messenger services enterprise, also providing instant games, sportsbook, and online casino. The appropriate KYC protocols and operational constraints have been adopted (as outlined below) to ensure the activities do not constitute an inordinate AML risk.

We carried out a comprehensive analysis of our customers, products, services, and delivery channels, as well as geographical risk factors with the help of the different teams in all our departments. To guide us through the process we used FATF recommendations as well as the experience built through years in the gaming market, where we had the opportunity to learn from the payment industry standards and through experience with different product providers. The outcome of our assessment

indicated that we are in line with the latest regulatory requirements as published in January 2025 by the GCB.

The Company's target demographic is the casual, recreational player and gaming enthusiast, which sets out the standard for our risk appetite. Most of our customers are middle-aged workers.

The Company identified the following risks regarding its products and services and has adopted the 'Risk Management Strategy' as outlined below in this section. The business has identified and assessed the following risk factors:

6.2 Business Services related risks:

The Company provides its customers with access to a variety of payment service providers to fund their accounts and with the capacity to hold their gambling balances to enable them to fund their betting at any time. We identify the risk of criminals being attracted to use our facilities for storing their money or use them to move money around to integrate them into the economic system.

6.2.1 Business Services risk factors:

Licensing: Licence revocation
Financial: Fraud and chargebacks
Technology: Cyber security threats
Technology: System downtime
Technology: Game integrity Issues
Consumer protection: Problem Gambling
Consumer protection: Underage gambling
Consumer protection: Data privacy issues

6.2.2 Mitigation and controls:

According to the attached risk matrix, the following risk mitigation and controls must be implemented:

License revocation: implementation of compliance programs to ensure compliance with applicable laws
Fraud and chargebacks: Ensuring implementation of fraud prevention processes including payment verification tools
Cyber security threats: Implementation of cyber security measures and screening
System downtime: Implementation of back up servers and processes to ensure up time
Game integrity issues: Ensuring integrity of games system through review of games certifications
Problem gambling: Ensuring appropriate monitoring of player activities through implementation of RG programs

Underage gambling: implementation of appropriate KYC process to ensure compliance
Data privacy issues: Ensuring implementation of data protection measures

6.2.3 Residual risk:

According to the risk matrix, regarding the residual risk that is left due to the risk mitigation and controls implemented, the following must be conducted to combat the residual risk:

License revocation: Implementing internal audit to ensure compliance by a Compliance officer
Fraud and chargebacks: Implementing internal audit to ensure compliance by a Compliance officer
Cyber security threats: Implementing random penetration testing by Internal Company's team
System downtime: Implementing internal audit to ensure compliance by a Compliance officer
Game integrity issues: Implementing internal audit to ensure compliance by a Compliance officer
Problem gambling: Implementing internal audit to ensure compliance by a Compliance officer
Underage gambling: Implementing internal audit to ensure compliance by a Compliance officer
Data privacy issues: Implementing internal audit to ensure compliance by a Compliance officer

6.3 Product related risks:

- Lottery products: Although it is recognised that lower amounts of cash can be laundered through a continued and sustained period of time, having regard to the nature of Company's target clients, the prizes and nature of the products render any significant money laundering scheme unworkable, as (even in the absence of our numerous safeguards) such limits would make any substantive money laundering effort logistically impractical. However, we identify the risk of 'Disposal' of money (or elimination of proceeds of crime)
- Instant Games: Like with Lottery products, the size of the prizes and nature of the products make any substantive money laundering effort impractical. However, we take into consideration the possibility of someone attempting to use these types of games for the disposal of criminal funds or layering the source if a prize is hit.
- Casino products: these products pose a greater risk for the use in laundering strategies such as layering:
- Slots: this product has a higher return for the player and volatility than the previously mentioned products, such poses the risk of being more useful for layering if a larger prize is hit. It can also be used for the disposal of funds.

- Virtual Casino: games offering low risk bets which could be used to generate betting activity whilst avoiding losing the funds, to then cashout the proceeds disguised as genuine casino wins.
- Live Casino: same as regular casino, it could be used to generate minimum betting to disguise funds. This product also offers games which enable customers to play on the same tables with customers from other casinos in the same network, thus it poses the risk of being abused to transfer funds from one account to another by purposely taking the wrong decisions during gameplay.
- Sportsbook: the ML risk from online sports gambling is similar to that seen in traditional casinos. An individual might collude with confederates on bets to hide the origin of funds, or a person could deposit money into a betting account and withdraw it after minimal wagering.

6.3.1 Product Risk factors:

The risk factors regarding product risk are the following:

Peer to peer gaming
Type of games allowing collusion between players
Bonus abuse - multi accounts
Game integrity vulnerability

6.3.2 Controls and implementation / residual risk:

The Compliance Officer must ensure the following regarding product risk:

- Ensuring KYC processes and linking accounts
- Ensuring only certified games are offered to players
- After implementation of controls, to combat the residual risk, the Compliance Officer will monitor activities related to product risk

6.4 Payment source related risks:

To responsibly identify and mitigate the risks inherent to the payment instruments which we accept, Company classifies potential deposit methods into three risk categories depending on the funding source:

6.4.1 Low risk – Negligible Source Risk

Level A (Negligible Source Risk) methods are payment instruments such as credit cards, debit cards, wire transfers, and direct deposit transfers where the source of funds is an account or credit facility, from a reputable country, and in the name of the customer, and that has been subject to the KYC processes of the financial institution or card issuer.

Such institutions and issuers are subject to rigorous regulatory oversight and AML compliance requirements, and as such it is the Company's assessment that the KYC of such institutions may be assumed to be unimpeachable for the purposes of the Company's operations. Therefore, Company regards the source risk of funds deposited by means of Level A methods to pose a Low ML/TF risk.

6.4.2 Medium risk – Managed Source Risk

Level B (Managed Source Risk) are such deposit methods as eWallets (e.g. Neteller, Astropay, etc.), pre-paid debit cards, and the like, where the deposited funds are transferred into an intermediary facility by the customer, and then subsequently used to purchase our products.

These could represent an extended risk if the eWallet or card issuer had unsatisfactory KYC, therefore enabling the transfer of funds that appear to be from the account holder, but which are not. In order to mitigate such risk, Company requires these processors to furnish a copy of their AML/KYC policies and procedures, which the Company shall review prior to implementation of such processing method to ensure that the AML/KYC processes are adequate.

Extended AML procedures may be introduced through the use of Level B deposit methods, as these pose a Medium Risk.

6.4.3 High risk- Moderate Source Risk

Level C (Moderate Source Risk) are deposit methods such as pre-paid gift cards, crypto currencies, or any "cash-like" wallets and methods where the funds are not from a readily verifiable originating source. The Company shall closely evaluate any such Level C deposit methods prior to implementation for potentially heightened AML and TF risk exposure. As there is no means to verify the source, in the event that the Company implements such deposit methods, the Company shall ensure that appropriate operational constraints are in place to warrant that the utility of such a potential means of money laundering is minimized or effectively eliminated. This may be accomplished by establishing rigorous deposit limits to logistically negate such deposit methods as an effective means of laundering funds, carrying activity assessments to identify unusual behavioural patterns, and/or such other constraints as it considers appropriate considering its risk assessment. We identify Level C methods as High Risk.

Where multiple sources of income, irregular income streams, or multiple payment instruments are identified in one account, this is also considered as posing a higher risk.

6.5 Customer related risks:

The customer risk assessment is categorized between the following risk area's:

Non-face to face relationship
Unverified, fictitious or front accounts

Anonymous accounts
High value depositing customers
False or stolen identity
Politically Exposed Persons (PEPs)
Adverse media
Dormant accounts
Source of Funds and/or Source of Wealth unknown for high spending customers
Changes to personal details for registered account holders
Drastic changes in deposit and/or betting behaviour
Use of multiple payment methods
Ownership mismatch of payment card/method
Duplicate/multiple accounts, same operator
Underage activity
Corporate/Third Party Accounts
Withdrawing without meeting play through requirements
Continuous low value activity to evade mandatory/regulatory thresholds and/or reporting
Open-loop transacting
Failure to undertake on-going customer monitoring
Failure to apply risk rating
Failure to change risk rating
Unusual activity
Suspicious activity

6.5.1 Mitigation and controls

According to the attached risk matrix, the following risk mitigation and controls must be implemented:

Non-face to face relationship: Ensuring registration process requires to input all information required to electronically verify player
Unverified, fictitious or front accounts ensuring implementation of processes to ensure it is possible to verify the correctness of information inputted
Anonymous accounts: Not to allow any anonymous account on the platform
High value depositing customers: Ensuring the correct flags are in place to carry out processes to verify the legitimacy of these payments
False or stolen identity: Implementation of verification method to obtain copies of ID, verify and reported stolen ID
Politically exposed person: Implement an appropriate PEP screening program
Adverse media: Implementing an internal risk assessment in the evaluate the level of risk in onboarding a customer the operator is willing to take
Dormant accounts: Implementing policies to ensure deposited funds are used for playing or flags are in place and ensuring closed loop

Source of funds: Request SOW and SOF in accordance with EDD policy published by the CGA
Changes to personal details for registered account holders Ensuring: a process is in place for verifying any new detail
Drastic changes in deposit and/or betting behaviour: Implementing player behaviours reviews
Use of multiple payment methods: Implement strict rules about payment methods allowed to one single player account
Ownership mismatch of payment card/method: Not allow deposits from card not belonging to the player
Duplicate/multiple accounts, same operator: Ensuring a KYC process in a place to link player accounts
Underage activity: Ensuring a KYC process in a place to link player accounts
Corporate/Third Party Accounts: Ensuring appropriate due diligence is carried out to identify correct level of risk
Withdrawing without meeting play through requirements: implementing player behaviours reviews
Continuous low value activity to evade mandatory/regulatory thresholds and/or reporting: Implementing player behaviours reviews
Open-loop transacting: Implementing strict rules for withdrawal and payment methods verification
Failure to undertake on-going customer monitoring: Implement periodic compliance audits
Failure to apply risk rating: Review risk assessment on a regular basis
Failure to change risk rating: Review risk assessment on a regular basis
Unusual activity: Ensuring experiences AML professional review activities to decide actions
Suspicious activity: Ensuring experiences AML professional review activities to decide actions

6.5.2 Residual risk

According to the risk matrix, regarding the residual risk that is left due to the risk mitigation and controls implemented, a compliance review will be conducted by a Compliance officer regarding the controls implemented corresponding to the applicable risk factor.

6.6 Geographical Risks

The geographical risk is the risk posed to the licensee by the geographical location of the business/economic activity and the source of wealth/funds of the business relationship. The nationality, residence and place of birth of an Account Holder have to be taken into account as these might be indicative of a heightened geographical risk. Countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction as well as countries which are known to have terrorist organizations operating within are to be considered as high risk. The opposite is also true and may therefore be considered as presenting a medium or low risk of ML/FT. In order to identify and manage potential hazards, the high-risk territories are the next:

- Prohibited Jurisdictions: these jurisdictions are prohibited under the Curaçao license conditions and/ or pursuant to a resolution of the Company's managing director;

- jurisdictions which are identified by FATF as high-risk jurisdictions subject to a call for action;
- jurisdictions under increased monitoring by FATF;
- countries which are identified by the European Union as high-risk countries;
- countries which are identified by the United States as state sponsors of terrorism.

6.6.1 Geographical Risk factors:

According to the attached risk matrix, the following risk mitigation and controls must be implemented:

Local legislation: Ensuring the creation of an appropriate risk assessment of the target jurisdictions
Sanction: Ensuring the creation of excluded territories list and sanction lists to ensure compliance
Source of funds: Ensuring the creation of an appropriate risk assessment of the target jurisdictions
Use of VPN: Implementing services for VPN unmasking
Incomplete player address : Ensuring appropriate registration flow and KYC to ensure correct amount of "hit" on different databases
Multiple locations/device: Monitoring device login and activities
Mismatch in country of residence and country of issuing card/bank account: Ensuring KYC processes and payment methods verification to detect mismatching

6.6.2 Residual risk

According to the risk matrix¹, regarding the residual risk that is left due to the risk mitigation and controls implemented, the following must be conducted to combat the residual risk:

Local legislation: Perform period reviews by Compliance officer
Sanction: Perform period reviews by Compliance officer
Source of funds: Perform period reviews by Compliance officer
Use of VPN: continue to review technological implementations by Internal Company's team.
Incomplete player address: Periodic review of databases and external resources by Compliance officer
Multiple locations/device: periodic review of databases and external resources by Internal Company's team
Mismatch in country of residence and country of issuing card/ bank account: Periodic review of databases and external resources by Compliance officer

¹ Attached Risk Matrix

7. SITE SUBSCRIBERS AND CUSTOMER ACCOUNTS (Website visitors Vs Account Registration)

7.1 Site Visitors/Marketing Subscribers:

We do collect data from potential customers who land on our site to help us grow our marketing database and increase our chances of customer acquisition and conversion.

When any individual first visits our websites, they must accept they are of legal age to bet and provide basic personal information before they can actually see the page contents. This is only a subscription, and the information will be used solely for marketing purposes, helping us promote our products and services and acquire a database of prospective customers whilst they have not yet made a decision on using the service. The information collected at this stage consists of:

- Full Name
- Email Address
- Password

Visitors also must accept our Terms and Conditions and Privacy Policy at this stage. These prospective customers will only be able to visit our pages and play demo-games.

7.2 Registering an account/Account Sign-up:

It is upon attempting a first deposit transaction, attempting to buy a product for the first time, or upon accepting one of our marketing offers sent to the subscriber's email address containing promotional gifts that the person will become a customer, an account will be registered for that person, and a relationship as such is established. Therefore, at this stage the prospective customer must provide the following information before they can proceed to make a transaction or accept our offer:

- Full residential address
- Date of birth
- Place of birth
- Nationality; and
- Identity number

8. CAPTURED DATA

Personal data is collected and treated by the Company as per our Privacy Policy published in our website, and in accordance with the laws of Curaçao.

8.1 Data inputted by the account holder on sign-up:

- full name
- permanent residential address
- date of birth
- place of birth
- nationality
- identity number
- Telephone number (optional)
- Alternative telephone number (optional)
- Email address
- Password

8.2 Data gathered silently:

- IP Address
- Device ID
- Device fingerprint
- Payment provider and third-party responses and alerts, including AVS checks, Verified by Visa, and MasterCard 3D Secure checks results.

8.3 Updates and Changes

If a customer requests a change to be made to his / her account details the following procedures shall be followed:

Via phone the client must be able to answer security questions associated with the account before updating address information. Via email client would need to submit a request with the new information and must also answer security questions associated with the account.

All name changes will require validated, documentary proof of change. The following are accepted as forms of verification of a name change:

- Marriage Certificate.
- Name Change Certificate; and/or
- Government issued identification

Address information can be updated online by logging into the account and making necessary updates. When a customer changes his/her address, it will be requested to submit a POA document. In case a customer is reported deceased, a copy of the death certificate is required.

With regards to updates in IP and device, our system automatically records these details with a time-stamp for every connection and transaction. This information is later used for further analysis.

9. KNOW YOUR CUSTOMER PROCEDURES - Customer Due Dilligence

Overview

Effective and consistently monitored KYC protocols are fundamental to mitigating payment risks, including payment fraud, ML, TF, and PF.

Customer due diligence is crucial for the Company to identify and verify the identity of its affiliates, service providers, and customers.

Because fraud and ML risks cannot arise until the initial transfer of funds begins, the Company initiates its due diligence, and enhanced due diligence (where necessary), at the point of the first attempted purchase. To achieve this, our Fraud Management System (FMS) monitors every transaction in real-time, applying configured rules to detect and mitigate risks associated with each customer account.

Current FMS rules include:

- Alerts to review newly registered customers.
- Velocity alerts based on the number and amount of purchases.
- Velocity alerts based on the number of registered payment instruments.
- Velocity alerts based on IP address.
- Alerts designed to trigger customer contact to confirm purchase details.
- Alerts and filters for discrepancies in customer details (e.g., registered country different from card issuing country, name on card does not match player's registered name).
- Filters to detect specific fraudulent scenarios based on historical data.
- Ongoing customer review alerts to re-evaluate an account's risk level over time. These include rules that detect increases in average deposits, tailored to individual customers to identify deviations from their usual spending patterns.
- Ongoing review alerts to enforce account verification or require updated verification documents for members whose spending reaches certain thresholds over time.

9.1 Identity Validation and Risk Assessment (Simplified DD)

Upon completion of a customer's first transaction, the Company conducts a verification check through our service provider using the ID document number provided by the customer during registration. This check is performed against government databases and, where available, returns confirmation of the individual's full name, date of birth (DOB), and address. Sanctions and Politically Exposed Persons (PEP) lists are also checked at this stage.

Risk scoring is applied during this process as well. To further ensure thoroughness, we review all newly created accounts daily using our reporting tools to verify data consistency and ensure that all accounts are reviewed.

9.2 Customer Due Diligence (CDD)

Following the identity validation and risk assessment described above, accounts identified as posing a higher risk will trigger the CDD process. This process limits the amount of funds a customer can spend before completing verification and automatically blocks the account if CDD is not completed within the specified timeframe.

In any case, customers meeting the following criteria are required to complete CDD. Their accounts will be frozen if they do not complete the process within 30 days of our request for verification documents:

- Customers engaging in financial transactions (single or multiple) equal to or greater than XCG 4000 (USD 2200).
- Customers requesting a withdrawal equal to or greater than XCG 4000 (USD 2200).

During the verification process, the account will remain blocked from further deposits and withdrawals until CDD is completed.

To fulfill CDD requirements, customers must provide clear copies of the following:

- A valid, unexpired government-issued document containing a photograph as proof of identity (passport, driver's license, ID card).
- Proof of address, such as a recent bank statement, utility bill (dated within the last 3 months), a letter from a public authority, or a rental agreement (dated within the last 6 months). For phone bills, only fixed-line bills are acceptable.
- Additional documentation may be requested until account verification is satisfactory.

If a customer does not comply with our requests within 30 days, the account will be fully frozen, and a report will be submitted to the Compliance Officer for review. If money laundering (ML), terrorist financing (TF), or proliferation financing (PF) is suspected, the customer will be reported to the FIU (Financial Intelligence Unit of Curaçao).

These documents are collected through a reputable service provider that verifies the legitimacy of submitted documents and collects biometric evidence from the customer. This service also monitors document expiry dates, enabling us to request updated documentation as needed.

Copies of the received documents are readily accessible to the Company at any time through the provider's portal. This provider is based in a low-risk jurisdiction that is not on any international high-risk or restricted country lists. The provider also adheres to its own compliance obligations and retains customer-uploaded documents indefinitely on our behalf.

9.3 Enhanced Due Diligence (EDD)

9.3.1 Overview

Certain customer relationships present heightened risks of money laundering, terrorist financing, or fraud. In these situations, the Company will perform EDD in addition to its standard customer due diligence procedures.

EDD involves taking additional steps to thoroughly identify the customer and their personal and financial background. These steps include:

- Obtaining further evidence to verify the customer's identity.
- Verifying specific aspects of the customer's identity, such as their occupation and the intended nature of the business relationship.
- Validating the source of funds to ensure they are attributable to the verified identity.
- Where necessary, establishing the customer's source of wealth.
- Enhanced proof of identity may be obtained through:
- Further research of customer information available in public databases, electoral rolls, the internet, and social media.
- Obtaining notarized copies of customer documents.
- Requesting proof of ownership of payment instruments, which may include:
 - Bank statements
 - Card statements
 - Credit card copies (with the middle 8 digits on the front and the CVV/CVC on the back obscured)
- Screenshots
- Transaction receipts
- Obtaining information on performed transactions and the intended nature of the business relationship.

If the source of wealth information cannot be adequately verified through public information, further evidence may be requested, such as:

- Personal savings account statements
- Employment paystips and/or pension statements
- Evidence of share sales and dividends
- Evidence of property sales, inheritances, gifts, or compensation from legal rulings
- Evidence of gambling winnings

All additional documentation is uploaded, encrypted, and stored electronically within our system, linked to the customer's account details. Customers subject to EDD must complete the verification process before they are permitted to withdraw funds.

The processing of this data is confidential and is performed by a select group of Company personnel who have received appropriate training and demonstrate the necessary technical skills, knowledge, and personal integrity to ensure confidentiality.

9.3.2 EDD Triggering Events

The circumstances that require Enhanced Diligence are where:

- A match against Sanctions or PEP lists. In this case the account will be frozen immediately, and no further business will be entertained. In case of a registered user who has become a PEP, this will be brought to the board to make a decision on whether we shall continue the relationship, ensuring tailored deposit limits are applied.
- Any FMS triggering event where following analysis a compliance agent reasonably perceives that there is sufficient grounds to suspect fraud, chargeback risk, money laundering, or the financing of terrorism or proliferation.
- A single transaction, or a series, combination or pattern of transactions involving USD 2200 (XCG4000 or equivalent) or more.
- A cashout in the amount of USD 2750 (XCG5000 or equivalent) or more.
- A single cashout request to a non-verifiable payment instrument.
- Any account activity that deviates from the usual behaviour of the regular customer.

Situations requiring EDD may be also reported to the Compliance Officer for further investigation.

Customers who already have documentation on file may be requested for updated documentation if details change on their account or the documentation becomes outdated, the Compliance department can at any stage request that the customer send in documentation to probe / reconfirm the customer identity, age and place of residence. At his discretion the Compliance Officer may require a customer's proof of identity to be notarised.

10. RISK MANAGEMENT STRATEGY

The Company's Fraud Prevention, Anti-Money Laundering (AML), and Counter-Terrorist Financing (CTF) protocols are predicated in three "Phases." These Phases, when considered as a comprehensive system, are designed to effectively mitigate potential financial risks associated with the Company's operations. The customer-specific risk assessment takes into account all relevant risk factors, including the player's overall profile and activity, alerts generated throughout the customer relationship, country or geographical area risks, and payment and product risks.

Throughout each Phase, the account's Risk Level is continuously reviewed and may be adjusted based on our findings. Each Phase is detailed below.

To support our risk management strategy, we utilize internal blacklists and our proprietary Fraud Monitoring System (FMS) software. The FMS is an internal risk management platform that enables us to identify and address risk scenarios through preconfigured alerts or "rules." This tool monitors all customer transaction activity and updates to customer account information. It is configured with rules that allow us to determine an account's risk level and take appropriate action, starting from the first

purchase attempt and continuing with every subsequent purchase. These actions can be automated or involve an agent analyzing triggered alerts and taking necessary steps based on the risk scenario. The system also uses historical data to identify known risk patterns.

In addition to the FMS, we use the data management provider Qlik to generate various reports, including daily reviews of accounts that made their first deposit on the previous day. We also use Qlik to search for similarities among accounts in our database during investigations.

10.1 General Principles

The Company adopts a risk-based approach and has implemented the following general principles to mitigate risks related to Money Laundering (ML), Terrorist Financing (TF), and Proliferation Financing (PF), considering the source, nature, and scope of our business channels and target markets:

- Company websites are blocked to countries listed as High-Risk Jurisdictions by the FATF, OFAC, and EU. High-risk countries are defined in regular statements by the FATF, OFAC, EU, and US INCSR, which we review periodically to assess customer account risk.
- All customer acquisition channels direct players to register directly on our website, ensuring all registering members are subject to our controls and procedures.
- Accounts of identified sanctioned individuals are immediately frozen, and the event is reported to the FIU of Curaçao.
- Anonymous or "numbered" accounts are strictly prohibited.
- New customer registrations are continuously monitored and matched within our database to identify potential duplicate or related accounts. Only one active account is permitted per customer and brand.
- Customer accounts must be held in the name of an individual. Accounts held by corporations, partnerships, trusts, associations, or other legal entities are not allowed. Customers explicitly agree to this condition upon registration and acceptance of our website's Terms and Conditions. If there is suspicion of an account being used by more than one individual, Enhanced Due Diligence (EDD) will be applied, and the account will be frozen if account ownership cannot be satisfactorily established.
- All account information and the identity of the account holder are verified through appropriate Know Your Customer (KYC) protocols (see Section 4 of this Policy) upon account creation, with each purchase, upon changes to personal information, and when a withdrawal is requested.
- All incoming payments must originate from verifiable sources associated with the member's identity. Third-party payment instruments are not accepted, and the registration of every payment instrument is monitored to detect this. If payment method ownership cannot be established, we take necessary steps to identify the true owner.
- Where possible, payout transactions are restricted to the payment instrument used for the initial purchase (i.e., funds are paid out only to the card, wallet, or other payment instrument used for the deposit). When a "closed loop" system is not possible, enhanced due diligence protocols are activated, including the production, review, and retention of identity-verifying documentation.

- All withdrawal requests are scrutinized, and account activity is reviewed before processing a payout. Player behavior and betting activity are reviewed, and withdrawals are categorized as a "prize" or "refund" for appropriate handling. Game providers are also asked to conduct their own checks on winnings.
- We only use game and payment providers from reputable jurisdictions who are also obligated to comply with AML, TF, and PF protocols.
- Cash transactions are prohibited.
- Credit is not extended to members under any circumstances.
- Intra-account transfers of funds or tokens, or any redeemable coupon or credit, are prohibited.
- Member activity is actively and continuously monitored for suspicious activity or changes in risk factors.
- All product purchases and transactions are electronic, recorded in detail, maintained, and auditable.

The Company does not, under any circumstances, create anonymous customer accounts or accounts under names known or reasonably suspected to be fictitious. We prohibit anonymous activity. All individuals must provide their details upon sign-up. Our system uses automated controls to detect duplicate information from previous registrations and to verify the uniqueness of each identity, thus enforcing appropriate limits on individual account profiles. These controls are supported by manual monitoring procedures.

Upon a customer's request, the Company will, unless legally obliged to do otherwise, return funds to the customer, sending the funds to a financial institution account held in the customer's name.

10.2 Phase 1 - Preliminary Screening (registration data assessment, identity validation, transaction activity monitoring, and Source confirmation):

This initial phase focuses on verifying the validity of the account holder's details and confirming that funds originate from a source verifiably belonging to the account holder. This process results in the assignment of a risk level to each customer's account, reflecting their risk profile.

The primary objectives are to:

- Establish the validity of the identity (i.e., its verifiability).
- Determine if the validated identity presents a heightened risk of fraud, terrorist financing, proliferation financing, or money laundering (ML).

Upon completion of the onboarding process and the creation of a new account, an automated preliminary screening is conducted. This screening identifies potential risk factors associated with the new registrant, and the account is assigned a corresponding risk level (Low, Medium, or High) based on the findings. Our systems may also automatically apply other actions to the newly created account, based on the identified risks and the results of initial checks with external databases.

A geographical location check is also performed. This check verifies that the customer's device IP country is within a permitted jurisdiction. Customers from non-permitted jurisdictions are informed that they cannot use the site.

Our automated rules also check for inconsistencies in country information, comparing the deposit IP country, registration country, and, where available, the country of issue of the payment instrument. This ensures that the details align and originate from a permitted jurisdiction. Sanctions and Politically Exposed Persons (PEP) lists are also checked during this stage.

In parallel, an automated screening is conducted to identify potentially linked or suspect account activity across all brands. Our automated search for duplicate and related accounts considers the following account details:

- Full Name
- Last Name
- Birth Date
- Zip Code
- Mobile Phone
- Landline
- Password Token
- Email address
- Transaction IP
- Login IP
- Bank Account
- Credit Card
- Other payment instrument identifiers

Further automated screenings search for and detect potentially suspicious elements, using preconfigured rules designed to identify various risk scenarios.

If any of these screenings identify potential issues, cases are automatically generated for Compliance Auditors to investigate and resolve, ensuring that business rules are applied appropriately. These rules may trigger various risk mitigation steps, including CDD, escalation to EDD, account closure, or limitations on account purchases and/or withdrawals. This preliminary screening also helps to detect and address potential bonus and affiliate abuse.

Depending on the account's risk level, triggering events, and the agent's analysis, actions or restrictions may be applied. These actions are commensurate with the level of risk; higher risks result in more restrictive measures. Examples include:

- Requesting user verification with documents.
- Calling the customer to clarify a situation.
- Blocking the account.
- Restricting purchases and/or payouts.

In cases of clear fraud and high-risk situations, a complete freeze of the account and refunding of customer purchases may be implemented to prevent further damage.

During the manual analysis phase, public records such as electoral rolls, social media, and property information may be used to enhance trust and partially verify the member's identity. Depending on the information found, identity validation may lead to immediate suspension of the account until full CDD is completed.

Accounts created with previously blacklisted details have their purchases restricted and are flagged for investigation and assessment by the Compliance team.

Furthermore, the Company automatically screens all credit card deposits against blacklists maintained by payment processors to detect fraudulent or stolen cards

10.3 PHASE 2 – RECURRING CONDUCT ASSESSMENT (On-Going Monitoring)

Monitoring of accounts for potentially suspicious activity, behaviour, or transactions (e.g. increased purchase amount, or member collusion) to mitigate the risk that an account holder conduct is intended to be fraudulent or to facilitate the surreptitious transfer of funds.

Customer monitoring is a continuous process that intensifies based on the risk level associated with an account. When circumstances allow, we may permit account holders to continue using our services while awaiting verification documents. However, any subsequent purchases made by these accounts will undergo close scrutiny, and we will proactively follow up until the account details are verified. Importantly, any withdrawal attempts from accounts pending verification are strictly prohibited without the explicit authorization of the Compliance team, which will only be granted after successful identity validation.

To ensure thorough risk management, a Compliance and Fraud Detection agent reviews both new and existing accounts through the FMS scrub. This process is crucial because risk levels can change, and new threats or scenarios may emerge. During the review, the agent applies internal business rules related to fraud prevention and security protocols.

The Company maintains ongoing monitoring of existing customer relationships and accounts. This includes:

- **Regular review of identification data:** Ensuring information remains current and relevant, particularly for high-risk registered customers or in cases of potential document fraud.
- **Optimized data management:** Maintaining identification data in a manner that facilitates continuous monitoring of each customer relationship.
- **Transaction scrutiny:** Analyzing financial transactions to confirm consistency with the Company's understanding of the registered customer and the account's risk profile.
- **Identification of dormant funds:** Generating reports to highlight account balances with no apparent transactional activity.
- **Triggered document refresh:** Requiring updated customer documentation upon reaching the following cumulative purchase thresholds (or equivalent in other currencies):
 - USD 10,000
 - USD 20,000
 - USD 50,000
- **Analysis of activity patterns:** Reviewing tournament results and promotional participation for potential connections between individuals.
- **Detection of collusive behavior:** Monitoring for any instances of customer collusion.

10.4 PHASE 3 – DESTINATION VALIDATION

The third phase of the Company's strategy to mitigate payment, ML, TF, and PF risks focuses on verifying the payout destination as belonging to the legitimate account holder.

Our primary payout policy for risk management dictates that withdrawals will only be processed back to the original payment method used for deposits (i.e., the same credit card, eWallet account, etc., from which the initial validated deposit was received). By ensuring that deposits originate from a verified individual and that payouts are directed back to the same verified individual, we significantly reduce the risk of AML for the organization.

Exceptions to the standard payout policy, where funds cannot be received by the original payment method (e.g., certain cards not accepting credits), require the customer to provide an alternative, verifiable payment method for withdrawals. In these instances, enhanced due diligence may be necessary before processing the payout. This includes a thorough investigation into the ownership of both the deposit and the proposed payout instruments.

10.4.1 Deposits and Withdrawals

All financial transactions, for both funding and withdrawing from a Player Account, must precisely match the name registered to the credit card or other payment accounts involved. Any discrepancies will be considered a breach of our Terms and Conditions, resulting in the suspension of the transaction and further investigation of the Player Account.

10.4.1.1 Deposits

Each Account Holder is required to use their own personal information and bank account for all transactions. The details provided on the deposit form must exactly match the information held by the Company.

Deposits into a Player Account are solely for the purpose of engaging in gameplay and using the Website's Services. Withdrawals are not permitted without prior wagering activity.

Furthermore, the Company does not provide interest on deposited funds. We also reserve the right to implement specific restrictions on payment methods in certain countries and/or for particular Players.

10.4.1.2 Withdrawals

An Account Holder is eligible to make a withdrawal request only after the initial deposit amount has been fully wagered and any specific bonus terms have been satisfied.

No withdrawal will be processed, and funds cannot be released from a Player's Account until the following conditions are met: (i) all required verification checks have been successfully completed; (ii) payments have been confirmed; and (iii) the Player has adhered to all other withdrawal conditions, specific rules, and promotional terms relevant to their use of the Website and/or their Player Account (including any applicable bonus requirements).

Withdrawal requests must be directed to the Account Holder registered on the Player Account and can only be processed to the same account from which the deposits originated. The information provided on the withdrawal form must precisely match the personal data held by the Company. Withdrawal requests made to third parties will not be honored and will result in account suspension and further investigation.

11. TRANSACTIONS USING CRYPTOCURRENCY

The Company adheres to the following mandatory requirements:

- **Client Due Diligence:** Collecting and verifying proof of identity and proof of address as previously outlined, ensuring the Player is at least 18 years of age.
- **Data Collection and Storage:** Collecting and storing data as detailed in the '(c) Captured Data' section.
- **Transparency Regarding Cryptocurrency:** Clearly stating in the Terms and Conditions, and highlighting, that cryptocurrency values are subject to significant market fluctuations.

Furthermore, it is crucial to understand that current anti-money laundering regulations mandate that Players may only deposit funds into their Player Account for the purpose of playing and utilizing the Services. Full verification of Players is required before any withdrawals can be processed. If funds are deposited without being used for gaming, we will request an explanation and inform the Player that we are not a banking institution. Repeated instances of such activity may lead to the Player's account being blocked. The Company is not a financial institution and does not provide interest on deposits.

The Company retains the unrestricted right to impose specific limitations on payment methods in designated countries and/or for individual Players.

Notifications regarding the introduction of new payment methods will be prominently displayed on the Website's homepage as they become available.

12. POLITICALLY EXPOSED PERSONS AND SANCTIONED INDIVIDUALS

We conduct regular screenings of our player database to identify Politically Exposed Persons (PEPs) and individuals subject to sanctions:

- **New Customer Screening:** All new customers are checked against global PEP and Sanctions lists upon their first deposit attempt.
- **Ongoing Monitoring:** Given the dynamic nature of these lists, all active customers undergo monthly checks to update their PEP and Sanctions status. An active customer is defined as an account holder with transaction activity within the preceding three months. Customers inactive for a longer period will be re-screened upon their next deposit or withdrawal attempt.

We utilize the services of a reputable third-party provider for these screening processes.

Identified sanctioned individuals will have their accounts immediately frozen, and their details will be reported to the Financial Intelligence Unit (FIU) of Curaçao via the goAML reporting portal.

If an existing customer becomes a PEP, the Company will conduct Enhanced Due Diligence (EDD). This includes identifying their specific public function, country of origin, and obtaining senior management

approval to continue the business relationship. Ongoing monitoring of the customer's activity will be implemented.

Should an existing customer, not initially identified as a PEP, subsequently become one, the relevant employee must conduct EDD and secure senior management approval within a thirty (30) day timeframe. Failure to do so will necessitate the termination of the business relationship with the customer.

To determine if an Account Holder (or their beneficial owner) is a PEP, we may obtain information directly from the Account Holder (e.g., through a standardized self-declaration form) or by using reliable electronic databases to screen our customer database. When relying on self-declaration, the employee is required to: (a) provide the Account Holder with a clear definition of a PEP; and (b) verify the provided information on a risk-sensitive basis.

13.SUSPICIOUS INCIDENTS (Unusual Transactions)

13.1 Identification

While a definitive list of Suspect Incidents is not possible, Compliance agents will investigate the following events, which may be considered suspicious for the purposes of this Policy:

- A customer makes a purchase, requests a cancellation, and then attempts a withdrawal to a payment method different from the one used for the deposit.
- A customer appears to be colluding with other account holders, or their behavior otherwise raises suspicion of money laundering (ML) or terrorist financing (TF).
- Customers become abusive and/or are unwilling to provide requested verification documents.
- A customer exhibits suspicious gaming or financial activity.
- Customers register accounts using unverifiable information.
- A customer attempts to use deposit methods that do not belong to them.
- Customers seek to deposit unusually large sums of money.
- Transactions or activity display unusual patterns lacking apparent economic or lawful purpose.
- Customers maintain account balances without any clear reason.
- Any behavior brought to the attention of the Compliance Officer, which they, using reasonable judgment and professional experience, deem suspicious or warranting further investigation.
- Transactions reported to the Police or the Department of Justice as potentially linked to money laundering or TF.
- Deposits or withdrawals totaling USD 2750 (XCG 5000) or more, whether in a single transaction or a series of related transactions.

13.2 Reporting of Suspicious Incidents to the Compliance Officer

Any significant Suspect Incident must be reported to the Compliance Officer immediately, along with a detailed description of the event that triggered the alert.

To report unusual transactions, the Compliance Officer can be contacted at any time via email at the dedicated mailbox: aml@litermi.com.

The Compliance Officer has unrestricted access to all customer information, records, and documents required to conduct a thorough investigation.

13.3 Investigation

The Compliance Officer is responsible for the prompt investigation of all significant Suspect Incidents.

As part of this investigation, they will determine if the incident necessitates reporting to the relevant authorities. Any accounts implicated in a Suspect Incident will remain blocked pending clarification, ensuring that individuals involved in the suspicious activity are not alerted.

Upon concluding the investigation, the Compliance Officer will thoroughly document their findings and, when appropriate, submit a suspicion report to the FIU. The Compliance Officer will also devise a specific, tailored plan of action for managing the customer's account in a way that avoids raising suspicion with the player.

14.REPORTING SUSPICIOUS INCIDENTS TO THE AUTHORITIES

Legacy Eight Curaçao N.V. as a Curaçao based company, has a mandatory reporting obligation of unusual transactions to the FIU Curaçao

If, after investigating a Suspicious Incident, the Compliance Officer determines that a report is required, the incident will be reported to the FIU of Curaçao via the goAML reporting portal. This report will include all relevant supporting evidence, related information, and a comprehensive explanation of the situation.

15.RECORD-KEEPING

Unless instructed otherwise by competent authorities, the Company will retain the original or a copy of the following documents (including electronic communications like email) in an easily accessible format for the specified minimum periods:

- **Transaction Documents:** A minimum of 5 years from the completion date of both the transaction and any related transactions.
- **Customer Due Diligence (CDD) Information:** All data used for customer identification, as well as any other files and correspondence related to the customer relationship, for at least 5 years after the individual ceases to be a registered customer.
- **Reports and Disclosures to the Compliance Officer:** For 5 years from the date the individual ceased to be a registered customer.
- **Training Records:** For 5 years from the date the training was conducted.

- **Internal Scrutiny and Investigation Findings:** Records of findings from internal reviews and investigations into customer backgrounds, transactions, or other activities (e.g., source of funds) for at least 5 years from the date the record was created.
- **Business Risk Assessment and Compliance Review Documents:** Minutes and other documents related to the Company's business risk assessment and reviews of its anti-money laundering and counter-terrorist financing compliance measures will be kept for 5 years from the completion date of the review, or until superseded by later documents.
- **Policies, Procedures, and Controls:** The Company's policies, procedures, and controls, including previous versions of relevant sections of its approved internal control system, will be retained for 5 years after they are no longer in effect.

Upon a legitimate request from competent authorities, the Company will provide records of player documents, detailed transaction history, CDD or Enhanced Due Diligence (EDD) information, and any other relevant data stored in our systems. We will maintain a log of the documents and information provided and retain a copy for our records.

In all circumstances, documents, CDD information, and EDD information will be made available promptly upon a valid request.

16.EMPLOYEE DILIGENCE

16.1 Employee Screening

To ensure the integrity of our compliance processes, every company employee or staff member is required to submit two professional references along with a recent police conduct or conviction record as part of their application.

Furthermore, we actively monitor and audit the system logs of employees responsible for conducting compliance checks.

We also maintain comprehensive mechanisms to log and track all actions and modifications made to customer accounts by our staff. These actions are fully traceable, and access to view sensitive customer data is restricted to key personnel only.

16.2 Personnel Training

Specific training on this Policy is mandatory for the following functional groups:

- Payment Risk Operations and Compliance agents
- Customer experience representatives
- Finance department representatives
- Supervisors and Managers
- Senior management and board of directors

This training will, at a minimum, cover:

- Guidance on identifying suspicious transactions and activities that must be reported to the Compliance Officer.
- Examples of various money laundering schemes that could potentially exploit the Company's services for illicit purposes.
- The Company's policies and procedures related to the awareness, detection, and prevention of Money Laundering, terrorist financing, proliferation financing, bribery, and corruption. Payment Risk Operations and Compliance agents will receive supplementary training on the latest ML/FT/FP updates, trends, and techniques, as well as specific ways our services could be misused for such activities.

The aforementioned training will be provided:

- Upon initial hiring or when an employee transfers into a relevant role.
- Whenever there are significant updates to this Policy.
- At least once every twelve (12) months of employment thereafter.

17.AUDIT FUNCTION

This program is monitored regularly in line with the regulations of Curaçao.

18.OTHER COMMENTS ON HANDLING PERSONAL DATA OF CUSTOMERS

Protecting member account details is paramount, and our staff adheres to the following strict guidelines:

- Member account details are exclusively discussed with the verified account holder.
- **Written Communication:** When contacting us in writing, users must use the email address registered to their account.
- **Telephone Communication:** When we contact customers by phone, the member is required to answer security questions related to their account details to verify their identity before any conversation about the account takes place.
- **Third-Party Disclosure:** Currently, no customer or transactional details are disclosed to any third party under any circumstances. Any future disclosure would only occur in strict compliance with the disclosure exemptions permitted under the laws of Curaçao or for the prevention or detection of crime when a legitimate request is received from a competent authority.