

# **4 AM QTF N.V.**

Willemstad, Curaçao

## **ANTI-MONEY LAUNDERING MANUAL**

Signature: *C. Drommond*  
Name: C. Drommond, Proxyholder of eMoore N.V.  
Date: March 20, 2026

# Table of Contents

|                                                                            |           |
|----------------------------------------------------------------------------|-----------|
| <b>REVISION HISTORY .....</b>                                              | <b>2</b>  |
| <b>1. INTRODUCTION .....</b>                                               | <b>3</b>  |
| 1.1. POLICY .....                                                          | 3         |
| 1.2. OBJECTIVE .....                                                       | 3         |
| 1.3. SCOPE.....                                                            | 3         |
| 1.4. OPERATING PROCEDURES .....                                            | 3         |
| 1.5. COMPLIANCE FUNCTION “CF” .....                                        | 4         |
| 1.6. INDEPENDENT TESTING AND AUDITING .....                                | 4         |
| 1.7. WHAT THIS MANUAL COVERS .....                                         | 4         |
| <b>2. WHAT IS MONEY LAUNDERING.....</b>                                    | <b>5</b>  |
| <b>3. REGULATORY FRAMEWORK.....</b>                                        | <b>5</b>  |
| 3.1. NATIONAL REGULATIONS.....                                             | 5         |
| 3.2. INTERNATIONAL REGULATIONS .....                                       | 6         |
| <b>4. RISK ASSESSMENT .....</b>                                            | <b>7</b>  |
| 4.1. OVERVIEW.....                                                         | 7         |
| 4.2. RISK ASSESSMENT .....                                                 | 7         |
| 4.2.1. <i>Business Risk Assessment (BRA)</i> .....                         | 7         |
| 4.2.2. <i>Customer Risk Assessment (CRA)</i> .....                         | 8         |
| 4.3. CLIENT ACCEPTANCE PROCEDURE .....                                     | 11        |
| 4.3.1. <i>Know Your Customer Procedure</i> .....                           | 11        |
| 4.3.2. <i>Client Due Diligence</i> .....                                   | 12        |
| 4.3.3. <i>Client Acceptance</i> .....                                      | 14        |
| 4.4. THE ROLE OF EACH EMPLOYEE, INCLUDING SUPERVISORS.....                 | 14        |
| 4.5. REPORTING OF UNUSUAL TRANSACTIONS .....                               | 14        |
| 4.6. POTENTIAL SUSPICIOUS ACTIVITY .....                                   | 15        |
| 4.7. INTERNAL UNUSUAL ACTIVITY REPORTING .....                             | 16        |
| 4.8. EXTERNAL UNUSUAL ACTIVITY REPORTING .....                             | 17        |
| <b>5. GOVERNMENT REQUEST FOR INFORMATION AND INFORMATION SHARING .....</b> | <b>17</b> |
| 5.1. SHARING OF INFORMATION .....                                          | 17        |
| <b>6. OPERATING PROCEDURES.....</b>                                        | <b>17</b> |
| 6.1. ACCOUNT OPENING PROCEDURES .....                                      | 17        |
| 6.2. ACCOUNT FUNDING PROCEDURES .....                                      | 18        |
| 6.3. ACCOUNT WITHDRAWAL PROCEDURES.....                                    | 18        |
| <b>7. RECORDKEEPING .....</b>                                              | <b>18</b> |
| <b>CONTACT INFORMATION.....</b>                                            | <b>19</b> |

**REVISION HISTORY**

| <b>Version #</b> | <b>Effective Date</b> | <b>Approving Official</b> | <b>Responsible Office</b> | <b>Next Review Date</b> | <b>Comments</b> |
|------------------|-----------------------|---------------------------|---------------------------|-------------------------|-----------------|
| 1.0              | February 20, 2026     | eMoore N.V.               | Compliance function       | February 20, 2027       | -               |
| 1.1              | March 20, 2026        | eMoore N.V.               | Compliance function       | February 20, 2027       |                 |

## **1. Introduction**

### **1.1. Policy**

It is the policy of 4 AM QTF N.V. (“the Company”) to prohibit and actively prevent money laundering, and any activity that facilitates money laundering or the funding of criminal or terrorist activities across any of the Company’s operations, and to comply with all national and international anti-money laundering (“AML”) requirements.

### **1.2. Objective**

The Company is a limited liability company, duly incorporated and registered in accordance with the laws of Curaçao. Its business regards the operation of a high-end pari-mutuel betting agency acting as an intermediary between The Hong Kong Jockey Club and exclusively, to elite high-stakes horse racing bettors wishing to access HKJC pari-mutuel betting pools. The business facilitates seamless wagering into HKJC pools through direct connection via Inter Tote Service Protocol (ITSP), ensuring transparency, efficiency and compliance with regulatory requirements.

This policy is written based on the national legislation on AML, Countering the Financing of Terrorism (“CFT”), and the penalization of predicate crimes of Curaçao, as well as applicable international standards set by the Financial Action Task Force (“FATF”). Combined, these regulations provide a solid and internationally accepted standard for the procedures the Company maintains to prevent the misuse of its Services. However, seen the specific nature of the services provided, the Company may deviate from the aforementioned legislation and regulation in that sense that it applies a stricter policy, for example on the moment of verification.

### **1.3. Scope**

The Company is committed to the highest national and international AML and CFT standards when providing its Services, and requires management and employees to follow these standards.

Under no circumstances will the Company engage in transactions involving customer funds, including, but not limited to, cash transactions.

### **1.4. Operating Procedures**

This Anti-Money Laundering Manual (“AML Manual”) is applicable to the scope of the services offered by the Company.

This Manual, and its AML program in general, enjoy the support of the management of the Company, all of whom strive to maintain a culture of compliance. Compliance with this AML Manual is a condition of employment. All employees are required to comply with the policies and procedures set forth herein, and play an active role in preventing the illicit use of the Company’s services and assets.

Failure to comply with the provisions of this manual may result in disciplinary action, including suspension and/or dismissal.

### **1.5. Compliance function “CF”**

The Company appoints a Compliance Function (“CF”) who will work with management to ensure that all of the Company’s matters subject to AML regulations are in compliance with applicable laws and regulations. The duties of the CF include, among other things, aiding in the monitoring of the Company’s overall compliance with AML obligations and overseeing a corporate AML policy, which duties necessitate communication concerning AML responsibilities and day-to-day compliance.

Most importantly, the CF works with management to assess and document the risks related to money laundering using the Company’s platform, while also documenting and implementing mitigation measures to address those risks.

The Compliance function is in charge of the periodical review of this manual and the required updates following any changes in the applicable legislation or operation of the Company.

Currently the office of the Compliance function is located at the address of Groot Kwartierweg 10, Willemstad, Curaçao.

### **1.6. Independent Testing and Auditing**

The Company recognizes that to maintain an effective AML compliance program it must implement an independent system to (i) verify that management and employees are following the policies and procedures set forth in this Manual, and (ii) detect any deficiencies in said policies and procedures. Consequently, at the discretion of the Company’s management and CF, or when necessitated by a significant change to the Company’s platform and/or operating environment, independent testing of the AML compliance program will be conducted by internal audit or qualified external consultants. This independent testing will be risk-based and tailored to the Company’s unique business model while covering all elements of the AML program, including, but not limited to, customer due diligence, transaction monitoring, required reporting, record keeping, and training. The Company will cooperate fully with all consultants and compliance reviewers, and with any federal and state regulatory examination staff throughout this process.

On completion of testing, the auditor/consultant will report its written findings to management and the CF, who will work together to address any resulting recommendations. Management will also document whether recommendations were followed and, if not, why not and what steps should be taken to address the issue.

### **1.7. What This Manual Covers**

This Manual describes the Company’s risk-based AML program, and includes the following:

- A description of what money laundering is, and the Company’s legal obligations to combat it;
- Relevant Curaçao AML legislation;
- Specific examples of money laundering;
- Overview of the officers responsible for implementing the AML program;
- Record keeping requirements applicable to the Company;
- Customer due diligence procedures (Know Your Customer);
- Internal controls, policies, and procedures to assure ongoing compliance; and
- Internal and/or external independent testing for compliance.

## **2. What is Money Laundering**

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds, such that unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets.

Money laundering occurs in three stages. Cash first enters the financial system at the “placement” stage, where the cash generated from criminal activities is introduced into a traditional or nontraditional financial institution, such as a casino, or into the retail economy. At the “layering” stage, the funds are transferred into a different form, institution, or account, typically through multiple complex financial transactions that conceal the true origin of the funds and eliminate any potential audit trail. At the “integration” stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Although money laundering is often associated with narcotic trafficking, it can also involve other types of criminal activity, including:

- Terrorism
- Bribery
- Extortion
- Organized Crime
- Racketeering (“RICO” (Racketeer Influenced and Corrupt Organizations Act))
- Fraud
- Forgery
- Counterfeiting Currency
- Smuggling
- Piracy
- Tax Evasion
- Transportation of Stolen Property

Importantly, although this policy is labelled an “anti-money laundering” policy, it is meant to broadly address prevention, detection, and reporting of all forms of illicit finance that occurs by, at, or through any of the Company’s components.

## **3. Regulatory Framework**

### **3.1. National regulations**

Pursuant to the National Ordinance of Money Laundering (1993), money laundering is a criminal offense in Curaçao. The country has instituted the following regulations to combat the threat:

- a) The Code of Criminal Law (Penal Code) (N.G. 2015, no. 74);

- b) The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G. 2015, no. 68 (NORUT) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- c) The National Ordinance on Identification of Clients when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2009, no. 66 (N.G. 2010, no. 40) (NOIS) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- d) The National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification of Clients when rendering Services. (National Decree containing general measures on Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70);
- e) National Ordinance on the Prolongation of the sanctions national decrees (N.G. 2018,34);
- f) 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);
- g) Sanctions national decree North Korea (N.G. 2015,30);
- h) Sanctions national decree Libya (N.G. 2015,28); and
- i) 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.

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, and other criminal activities.

### **3.2. International regulations**

As a member of the FATF ([www.fatf-gafi.org](http://www.fatf-gafi.org)) and of the Caribbean Financial Action Task Force ([www.cfatf-gafic.org](http://www.cfatf-gafic.org)), Curaçao is meeting international standards by regularly incorporating the principles propagated by these organizations into the country's national legislation.

On an international level, the FATF plays a very important role in combating money laundering, terrorist financing, and the proliferation of weapons of mass destruction by encouraging its member counties (39 direct members & 180 affiliates as of June 2023) to comply with AML & CFT best practices. In doing so, the FATF collaborates with similar international organizations.

The Company's current AML policy is informed by the FATF as well as more localized rules regarding AML/CFT compliance. This ensures that the policy is rooted in internationally accepted best practices while maintaining the flexibility to address unique challenges facing Curaçao companies.

## 4. Risk Assessment

### 4.1. Overview

The Company's AML program is built around management's/the CF's assessment of individualized AML/CTF risks facing the Company given its unique combination of services, customers, and geographic locations.

### 4.2. Risk Assessment

The Company has conducted a risk assessment to identify the ML/TF risks it is possibly and realistically exposed to, to ensure that the policies, controls and procedures it adopts are adequate to prevent and mitigate these risks.

#### 4.2.1. Business Risk Assessment (BRA)

The Company conducted a comprehensive business risk assessment to identify its risks and manage them accordingly. The table below presents the identified risks, their corresponding categories, their likelihood, potential impact and overall risk score

| Risk ID | Risk                                                 | Risk Category        | Likelihood | Impact | Risk score (LxI) |
|---------|------------------------------------------------------|----------------------|------------|--------|------------------|
| R001    | Breach of licensing terms in any jurisdiction        | Regulatory & legal   | 1          | 5      | 5                |
| R002    | Failure to comply with AML/CTF regulations           | Regulatory & legal   | 2          | 5      | 10               |
| R003    | Non-compliance with responsible gambling regulations | Regulatory & legal   | 2          | 4      | 8                |
| R004    | DDoS attack disrupting platform access               | Cybersecurity        | 2          | 5      | 10               |
| R005    | Data breach or data loss                             | Cybersecurity        | 3          | 5      | 15               |
| R006    | Unauthorized access to customer data                 | Cybersecurity        | 3          | 5      | 15               |
| R007    | System outages or downtime during peak events        | Operational          | 3          | 5      | 15               |
| R008    | Dependence on third-party software or platforms      | Operational          | 4          | 3      | 12               |
| R009    | Negative media coverage or scandals                  | Reputation           | 4          | 5      | 20               |
| R010    | Players developing gambling addiction                | Responsible Gambling | 1          | 5      | 5                |
| R011    | Failure to intervene with at-risk players            | Responsible Gambling | 2          | 4      | 8                |

#### Mitigation strategy and residual risk

The following tables show the mitigation strategy to be implemented and the effectivity rate, followed with the activities to reduce residual risk, the residual risk score and the 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    | Close monitoring of customers, by support  | 10                               |

|      |                                    |    |
|------|------------------------------------|----|
| R004 | Cloudflare, WAF, redundancy        | 9  |
| R005 | Encryption, multi-layer security   | 12 |
| R006 | Role-based access control, 2FA     | 9  |
| R007 | Load testing, cloud infrastructure | 9  |
| R008 | SLA enforcement, redundancy plans  | 7  |
| R009 | Crisis communication plan          | 12 |
| R010 | Close continuous monitoring.       | 9  |
| R011 | Close continuous monitoring        | 5  |

| Risk ID | Activities to reduce Residual risk                                         | Risk score (LxI) | Residual risk score | Residual risk level |
|---------|----------------------------------------------------------------------------|------------------|---------------------|---------------------|
| R001    | Continuous license compliance training, implement internal reviews         | 5                | 1*                  | Low                 |
| R002    | Enhance KYC processes, deploy AI for transaction monitoring                | 10               | 1*                  | Low                 |
| R003    | Inquire customer feedback                                                  | 8                | 1*                  | Low                 |
| R004    | Set up DDoS scrubbing service, automate scaling responses                  | 10               | 1                   | Low                 |
| R005    | Conduct periodic penetration testing, enforce data classification policies | 15               | 1*                  | Low                 |
| R006    | Monitor admin activities                                                   | 15               | 6                   | Medium              |
| R007    | Use high-availability architecture, incident response planning             | 15               | 6                   | Medium              |
| R008    | Initiate guided interventions                                              | 12               | 5                   | Medium              |
| R009    | Media monitoring, train spokespersons, prepare PR statements               | 20               | 8                   | High                |
| R010    | Install automated alert systems, limit manual overrides                    | 5                | 1*                  | Low                 |
| R011    | Inquire customer feedback                                                  | 8                | 3                   | Low                 |

\*Hard Floor Cap applied

The Company is in the process of developing a technological development risk assessment statement which should be regarded as an addition to this policy.

#### 4.2.2. Customer Risk Assessment (CRA)

The Customer Risk Assessment evaluates the risks the Company may encounter when providing services to clients. Due to its specific nature of business, the Company conducts the CRA before establishing a business relationship. This procedure aims to detect, mitigate and deter money laundering, terrorism financing, and proliferation financing risks (possibly) associated with each potential customer at an early stage. Regular personal and direct contact with clients further facilitates regular assessment of player activity.

##### Risk areas

The Customer Risk Assessment covers four areas:

- Customer risk,
- Transaction risk (funding methods),
- Interface risk,
- Geographical risk

### Customer risk

This risk assesses the money laundering or terrorism financing risk related to the provision of services to clients. Insufficient customer risk assessment can result in the acceptance of clients with the intention to misuse the Company for money laundering, terrorism financing or proliferation financing. Activities or situations indicating a high customer risk include but are not limited to the following:

- Nature of income: multiple unclear and/or dubious source of income.
- Politically Exposed Persons (PEPs).
- Use of third parties or accounts from others.
- Anonymous behavior or false identity.

### Product, Service 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 business model of the Company does not involve any gaming software. The Company acting as an intermediary agent between HKJC and the bettors, will not manage the wagering platform. The wagering is effectuated by means of direct communication between the Company and the player through a tote system and the use of ITSP, securing the connectivity and direct placement of a wager onto the HKJC platform. Its service would be the administrative registration of the wagering activities.

Risks in relation to the Product and service would be primarily on operational level and are covered in a separate policy.

Furthermore, due to the high roller status of the players and the considerable amount transferred at the commencement of the business relation, no other funding method is accepted than bank transfers.

The Services of the Company are provided through a set API, ensuring the protected communication between the Player and the Company.

### Interface risk

The method used to establish a business relationship or conduct transactions can affect the risk level.

The business model of the Company maintains a personal level approach. Prospect players are contacted personally via web calls or personal meetings. Legal representations and anonymity is not accepted.

The wagering is further effectuated through the exclusive use of a tote system supported by ISTP. This ensures the direct connectivity between the client and the HKJC for the direct placement of a wager. The Company will keep a register of the wagering activity and the available balance.

### 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 client'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 are regarded as high risk.

Noting the Company's specific nature of business it will not accept clients from jurisdictions of high risk for ML/TF purposes.

The following countries expose the Company to high geographical risk:

- Countries on the FATF list of High risk jurisdictions subject to a Call for Action;
- Countries under OFAC/EU/UN sanctions
- High corruption of terrorist funding regions

Customers who are residents of or transact from a country mentioned in one of the situations above will not be accepted.

As follows an overview of identified risks.

| Risk ID | Risk                                             | Likelihood | Impact | Risk score (LxI) |
|---------|--------------------------------------------------|------------|--------|------------------|
| CR001   | Onboarding of Politically Exposed Persons (PEPs) | 1          | 5      | 5                |
| CR002   | High spenders without clear source of income     | 1          | 4      | 4                |
| CR003   | Unusual transaction behavior                     | 4          | 5      | 20               |
| CR004   | Customers from high-risk jurisdictions           | 3          | 5      | 15               |
| CR005   | Use of proxy or VPN to mask location             | 1          | 4      | 4                |
| CR006   | Frequent disputed transactions                   | 1          | 4      | 4                |
| CR007   | Inconsistent user behavior                       | 1          | 5      | 5                |

### 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 |
|---------|--------------------------------------------------------------------|----------------------------------|
| CR001   | EDD, SOF/SOW checks, PEP list screening                            | 9                                |
| CR002   | Income verification, affordability checks                          | 12                               |
| CR003   | Real-time transaction monitoring, behavior-based                   | 12                               |
| CR004   | EDD for high-risk countries, risk profiling                        | 9                                |
| CR005   | Detect VPNs, additional KYC                                        | 10                               |
| CR006   | Monitor payment patterns                                           | 7                                |
| CR007   | Behavioral analytics, device change alerts, step-up authentication | 9                                |

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

| <b>Risk ID</b> | <b>Activities to reduce Residual risk</b>                               | <b>Risk score (LxI)</b> | <b>Residual risk score</b> | <b>Residual risk level</b> |
|----------------|-------------------------------------------------------------------------|-------------------------|----------------------------|----------------------------|
| CR001          | Automated PEP screening, periodic KYC updates                           | 5                       | 1*                         | Low                        |
| CR002          | Integrate Open Banking APIs, flag risky customer profiles               | 4                       | 1*                         | Low                        |
| CR003          | Machine learning models for velocity detection and layered transactions | 20                      | 8                          | High                       |
| CR004          | Review and update high-risk country lists, real-time geolocation alerts | 15                      | 6                          | Medium                     |
| CR005          | Deploy VPN/proxy detection tools, require manual verification           | 4                       | 1*                         | Low                        |
| CR006          | Monitor for fraud patterns, blacklist frequent abusers                  | 4                       | 1*                         | Low                        |
| CR007          | Trigger step-up verification on anomalies, lock compromised accounts    | 5                       | 1*                         | Low                        |

\* Hard Floor Cap applied

### 4.3. Client Acceptance Procedure

The Company has set standards determining whether a prospective customer can be accepted as a customer. Due to its specific nature of services, the Company opts for a more control-based approach implementing a high level of due diligence on all prospect clients based on its risk appetite.

Customer identification and verification is conducted before entering into a business relationship. Information and documentation is collected to establish and verify the identity, assess their profile, and confirm that they comply with AML TF regulatory, legal and regulatory requirements.

The following procedure is followed:

- Know Your Customer Procedure
- Client Due Diligence
- Client acceptance

#### 4.3.1. Know Your Customer Procedure

Customers are introduced through existing customers. Following the notification of application, the Company sets up a (virtual or in-personal) meeting to know the client and make inquiries about his/her background. Prospect customers must thereafter provide the following information to establish the identity:

- a. First and last name;
- b. Date of birth;
- c. Place of birth;
- d. Nationality;
- e. Residential address
- f. Government issued document of identification.

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

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

Additional information requested are (in so far not provided yet):

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

Further investigation is warranted if information is obtained indicating the customer:

- Has financial fiduciary duties (e.g., trustee, accountant, attorney, nonprofit/charity executive) that may create a risk of misappropriation or other illicit financial activity;
- Is associated with individuals or entities known to relate to the illicit generation of funds;
- Is a politically exposed person (PEP);
- Claims connections with businesses that have no actual operations; or
- Is the subject of substantial tax liens or has recently gone through bankruptcy.

The Company commissions an independent investigatory firm to perform a background check. The background check includes, but is not limited to, the following: verification of address, residency, and social security number (or applicable foreign ID number); inspection of public records (i.e. criminal records, sanction lists, etc.); and verification of good standing regarding OFAC matters, US terrorism watch lists, and banking sanctions.

The Company conducts a PEP check and Sanctions list check. Upon a possible hit, the onboarding procedure will be stopped and the prospect will not be accepted.

#### **4.3.2. Client Due Diligence**

The Company's approach to AML is driven by identifying potential clients and transactions that pose the greatest risk of money laundering prior to onboarding to immediately decide upon their acceptance as a client or rejection. Due to the specific nature of business i.e. small amount of elite high stakes bettors wagering considerable amounts, the Company conducts the same level of due diligence on all prospects and accepted clients i.e. a standard due diligence, covering the same risk appetite **prior** to the business relation and during its course.

Prospects have to provide a valid, government-issued photo identification (driver's license, passport, alien registration card, state issued ID card) and a permanent address. PO box addresses are not acceptable.

Verification of identity is conducted prior to onboarding. Since the business model requires the deposit of a sum surpassing the legal threshold of XCG 4.000. For this reason the Company establishes the identity and conducts the verification thereof prior to onboarding

The Company will further assess the indicated source of funds to determine whether this is derived from illegal activity or not. This may include querying third party databases, investigating if the prospect has sources of wealth/income commensurate with their wagering activity, and ascertaining whether the prospect has provided the Company with identification information or business-related information that can be readily confirmed.

If the provided information is considered unsatisfactory or is suspected to be fraudulent or obtained from a third party to perform illegal operations, the Company will decide to engage further background investigation methods or to terminate the onboarding process.

Due to the close and continuous contact with clients, the Company is able to conduct regular review of each client during the course of the business relation. If the Company becomes aware of any suspicious situation, it reserves the right to restrict the client from withdrawing funds from its account and/or prevent access to all or certain parts of the services and conduct investigation on the matter deemed suspicious.

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

As mentioned in Section 4.1 above, the Company conducts a control-based approach due to its specific nature of business. Between the first introduction and following onboarding period, the Company analyzes its clients to assess the related risk based on the initially collected information and the conducted PEP- and Sanctions checks. Due to the low risk appetite of the Company, any clients representing a high risk will be rejected.

#### High risk Individuals

The Company has determined the following customer categories to represent a high risk of ML/TF/FP. If during the prospect review the Company becomes aware of any of the following circumstances/ situations, it will immediately decide to reject the application.

If during the regular reviews any of these instances is identified, the Company will proceed to terminate the relation and will decide to report if so desired

- Minors

An individual cannot make use of the Services unless that individual is over twenty one (21) years of age. No underage individual will be accepted as a client.

- Anonymous accounts

At registration an individual is required to provide his/her full name as well as further personal information. The Company will not accept a prospect without having been provided with the personal information and verification documentation.

A client can only wager on its own behalf, not for other individuals nor for legal persons.

- Sanctioned individuals

The Company screens all applicants against international sanctions lists in order to prevent sanctioned individuals from opening an 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 acceptance or in case of a later listing, proceed to block the account. The case will then be escalated to Senior Management/ CF for further investigation and if required, reporting to the FIU.

- Residents from Restricted Jurisdictions

The Company will not accept residents of Restricted Jurisdictions.

- Politically Exposed Persons (PEP)

The Company will conduct a PEP and sanctions screening prior to onboarding. Upon the identification of a PEP, the Company immediately proceeds to perform further due diligence, to confirm the relevancy. This entails having to determine whether a prospect is a PEP or otherwise.

Depending on the outcome the application will be rejected or escalated to Compliance or Senior Management for further investigation and possible reporting to the FIU. The Company will not accept PEPs as a ground rule.

As mentioned screening for PEP status is carried out prior to the onboarding. Should a client who had not been identified as a PEP in the on-boarding stage result to have become one, the Company will implement the following measures within a thirty (30) day window failing which it will have to terminate the business relationship with the client:

- i. verify the identity and available details against certain (public or private) databases; and/or
- ii. request to provide information/ documentation showing source of funds/wealth.

#### **4.3.3. Client Acceptance**

Following the external investigation, the Company will complete an Account Holder Risk Assessment Form and will decide upon the acceptance or rejection of the prospect as a client. The procedure as described in Section 6.1 below, will be followed.

#### **4.4. The Role of Each Employee, Including Supervisors**

The Company's employees should look for patterns of client behavior that may suggest the risk of money laundering. Employees should look for a client's departure from his or her ordinary pattern of wagering, and should scrutinize suspicious transactions that cannot be readily explained.

Some examples:

- A client's betting activity increases significantly without explanation.
- A client appears to be coordinating his gaming with another client(s).
- A client abruptly changes the methods used for withdrawing funds, or unexpectedly uses multiple sources/destinations for funds.
- After the initial deposit, client has little to no play before requesting withdrawal.

In any of these or similar unusual or suspicious activities, the Employee should escalate the matter to the Senior Management or CF.

#### **4.5. Reporting of unusual transactions**

In accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Company is required, to detect and report either intended or completed unusual transactions. Following the monitoring of the player activities the Company is able to detect whether an activity or series of activities is unusual compared to the expected activities of the player. The NORUT has established objective and subjective indicators through which a service provider must determine whether client's transaction qualifies as an unusual transaction that should be reported to the FIU.

### Objective indicators

This mentions the circumstances which should be considered unusual and should be reported to the FIU. 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 client;
  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

A subjective indicator entails any activity that gives reason to assume it could be related to money laundering or the financing of terrorism or proliferation financing where there are any grounds for suspicion (or knowledge) of money laundering, terrorist financing,.

Any unusual transactions or circumstances for which the Company has not received sufficient explanation may necessitate a report to the FIU in Curaçao. The Company will hold a list of all instances in which it did not consider it necessary to report to the relevant authority. The decision not to report will need to be sufficiently supported.

## **4.6. Potential Suspicious Activity**

Regulators have identified certain suspicious activities that may occur in gaming and wagering facilities that may invite further internal inquiry and trigger reporting obligations. The following list is not exhaustive, and any determination of what may constitute suspicious activity will vary depending on the specific circumstances, the identity of the customer, and the nature of the particular transaction.

Applicable red flags that signal possible money laundering or terrorist financing include, but are not limited to the following:

- Minimal gaming despite the considerable deposit;

- Requests for structuring of transactions to stay at or slightly below reporting thresholds;
- A transaction that has no apparent business related or lawful purpose;
- Presenting a third-party check or wire transfer – whether apparently deriving from a business or an individual – for use in gambling-related activity.
- A prospect refuses to provide required information or identifying information;
- A prospect or client requests information about how to avoid regulatory reporting requirements;
- Law enforcement agencies deliver to the Company, a formal request for records, such as a subpoena, or make informal inquiries concerning the client;
- News articles or other media reports alleged acts of financial wrongdoing by a client;
- A client raises his or her financial transactions to levels well above the ordinary levels for that client;
- A client requests establishment of an account in the name other than the one by which the Company knows the client;
- A client attempts to deposit front money or to make payments using complex means, such as multiple source of funds or multiple methods of transmission, which could mask the source of the funds transmitted;
- A client presents funds which the Company has a basis for suspecting to be the proceeds of illegal activity;
- A client furnishes a legitimate type of identification document the Company believes is false or altered (e.g., address changed, photograph substituted) in connection with the completion of a report or another regulatory requirement;
- A client offers a bribe in the form of a tip or gratuity to an employee, or requests that an employee structures a transaction to evade the filing of a report;
- A client exhibits unusual interest in the Company's reporting policies or inquiries about how the Company's business day is calculated.

#### **4.7. Internal Unusual Activity Reporting**

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 CF, 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, collected customer information, and monitoring findings;

- Be documented in a confidential manner, using internal reporting tools or forms as determined by the CF.

#### **4.8. External Unusual Activity Reporting**

Upon receipt of an internal unusual activity report, the CF shall determine whether the reported activity is categorized as an objective- or subjective indicator and should further review all relevant information, including:

- Client identification and verification records;
- Transaction data and behavioral indicators identified through monitoring activities;
- Risk factors identified through the conducted risk assessment.

Where the CF establishes a transaction to be falling under the scope of an objective indicator or further determines a transaction to be related to money laundering, terrorism financing or proliferation financing, the CF shall proceed to file a report with the FIU in accordance with the NORUT, as referenced in Section 3.1 National Regulations.

External reporting shall:

- Be submitted without undue delay following the determination of suspicion;
- Be made exclusively by the CF or a formally designated alternate;
- Include all relevant and available information required by the FIU.

The CF shall ensure that:

- All submitted reports and supporting documentation are retained;
- Decisions not to report are sufficiently supported, properly documented and retained;
- Ongoing monitoring continues where appropriate, unless otherwise instructed by competent authorities.

### **5. Government Request for Information and Information Sharing**

#### **5.1. Sharing of Information**

Where permitted by law, the Company may share information about client(s) suspected of terrorist financing and money laundering with other financial institutions so that these institutions can identify said client(s) when determining whether to engage in business with them.

### **6. Operating Procedures**

#### **6.1. Account Opening Procedures**

Prospective clients must be introduced or referred to the Company's management by an existing client or a known reliable source. Only if a prospective client successfully completes the account opening procedure, they will become a Player. Prospective clients must submit the following to management before an application for a wagering account can be reviewed and potentially approved:

- (1) name;
- (2) date of birth (for an individual);
- (3) address; and
- (4) an identification number, which will be a Social Security number (for U.S. persons), or one or more of the following (for non-U.S. persons): a passport number and country of issuance, or other similar identification number, such as an alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard.
- (5) Brief biography
- (6) Signed Wagering Account Application
- (7) Signed Terms & Conditions Agreement
- (8) Signed Rules & Regulations Agreement

## **6.2. Account Funding Procedures**

Prospective clients must send funds to the Company via wire transfer or through personal check deposit for the purpose of opening a new wagering account. The funds must come from the personal account of the prospective client and are traced by management to verify compliance. All incoming funds are held in the Company's accounts. No cash transactions are allowed at any time, and any deviation from the procedures outlined in this will disqualify the prospective customer.

## **6.3. Account Withdrawal Procedures**

If approved for a wagering account, each client is assigned a unique TRA code. The TRA code is used by the Company to monitor customer's wagering activity for suspicious behavior. Requests to withdraw funds from a wagering account will only be considered if sent directly to management by the applicable client through a verified email address or other authorized messaging service. If the withdrawal request is duly received and verified, a bank wire can be organized by management and forwarded directly to the customer's verified personal account. Control over, and access to, the client's bank funds is restricted to the Company's management and ownership.

Enforcement of the procedures outlined in this Section is the responsibility of the Company's management. Strict adherence to these policies is required, and any deviation from their terms, or any other suspicious activity, will be reported immediately by management to the appropriate authorities.

The Company strictly adheres to the policies referenced in this Section, and any deviation from their terms, or any other suspicious activity, will be reported immediately by the Company's management to the appropriate authorities.

## **7. Recordkeeping**

The Company follows industry best practices in maintaining records of customer transactions for a minimum of five (5) years. If legally appropriate, the Company may provide copies of its records to the relevant authorities in connection with an AML/CFT related investigation.

### **Contact Information**

For any questions regarding this policy, please contact:

iGamingcompliance Curaçao N.V.

Groot Kwartierweg 10, Livestrong Building

Willemstad, Curaçao

Telephone: +599 9 462 1010

Email: [igamingcompliance@the-emgroup.com](mailto:igamingcompliance@the-emgroup.com)

This Policy has been approved as per the most recent effective date written above by:

eMoore N.V.

Statutory Director of 4 AM QTF N.V.



---

Name: C. Drommond

Function: Proxy holder eMoore NV

Date: 20/03/2026

Compliance Officer



---

Name: D. Mc Kenzie

Function: Compliance Officer

Date: 20/03/2026