

4 AM QTF N.V.

Willemstad, Curaçao

ANTI-MONEY LAUNDERING MANUAL

Table of Contents

REVISION HISTORY	2
1. INTRODUCTION	3
1.1. POLICY.....	3
1.2. OBJECTIVE	3
1.3. SCOPE	3
1.4. OPERATING PROCEDURES.....	3
1.5. MONEY LAUNDERING REPORTING OFFICER “MLRO”	3
1.6. INDEPENDENT TESTING AND AUDITING	4
1.7. WHAT THIS MANUAL COVERS	4
2. WHAT IS MONEY LAUNDERING	4
3. REGULATORY FRAMEWORK.....	5
3.1. NATIONAL REGULATIONS.....	5
3.2. INTERNATIONAL REGULATIONS.....	6
4. RISK ASSESSMENT.....	6
4.1. OVERVIEW	6
4.2. THE ROLE OF EACH EMPLOYEE, INCLUDING SUPERVISORS	6
4.3. CUSTOMER DUE DILIGENCE	7
4.4. REPORTING OF UNUSUAL TRANSACTIONS	7
4.5. POTENTIAL SUSPICIOUS ACTIVITY	8
4.6. INTERNAL UNUSUAL ACTIVITY REPORTING	9
4.7. EXTERNAL UNUSUAL ACTIVITY REPORTING	10
5. GOVERNMENT REQUEST FOR INFORMATION AND INFORMATION SHARING	10
5.1. SHARING OF INFORMATION.....	10
6. OPERATING PROCEDURES	10
6.1. ACCOUNT OPENING PROCEDURES.....	10
6.2. ACCOUNT FUNDING PROCEDURES.....	11
6.3. ACCOUNT WITHDRAWAL PROCEDURES	11
7. RECORDKEEPING	11

REVISION HISTORY

Version #	Effective Date	Approving Official	Responsible Office	Next Review Date	Comments
1.0	February 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. 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.

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. Money Laundering Reporting Officer “MLRO”

The Company appoints a Money Laundering Reporting Officer (“MLRO”) 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 MLRO 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 MLRO 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.

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 MLRO, 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 MLRO, 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 specific to account waging entities 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 (in the Company's case, typically gambling winnings).

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) and of the Caribbean Financial Action Task Force (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 MLRO's assessment of individualized AML/CFT risks facing the Company given its unique combination of services, customers, and geographic locations.

4.2. The Role of Each Employee, Including Supervisors

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

Some examples:

- A customer's betting activity or his financial transaction activity increases significantly without explanation.
- A customer appears to be coordinating his gaming with another customer(s).
- A customer abruptly changes the methods used for depositing/withdrawing funds, or unexpectedly uses multiple sources/destinations for funds.
- A customer funds his/her account in large amounts and has little to no play before withdrawing these amounts.

IF YOU SEE SOMETHING SUSPICIOUS, SAY SOMETHING TO YOUR SUPERVISOR.

4.3. Customer Due Diligence

The Company's approach to AML is driven by identifying customers and transactions that pose the greatest risk of money laundering so that such customers/transactions can be more carefully scrutinized, when appropriate.

Customers have to provide valid, current, 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.

For high-volume customers or transactions identified as having potential AML risk, the Company should attempt to assess the customer's source of funds to determine whether they derive from illegal activity. This may include querying third party databases, investigating if the customer has sources of wealth/income commensurate with their gaming activity, and ascertaining whether the customer has provided the Company with identification information or business-related information that can be readily confirmed.

Further due diligence may be 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.

4.4. 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 a transaction or series of transactions is unusual compared to the expected activities of the player. The NORUT has established objective and subjective indicators through which an operator must determine whether a player's transaction qualifies as an unusual transaction that should be reported to the FIU.

Objective indicators

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

The objective indicators are:

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

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

Subjective indicators

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

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

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.

4.5. 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, including the amount of the transaction, the identity of the customer, and the nature of the particular transaction.

Red flags that signal possible money laundering or terrorist financing occurring on the Company's platform include, but are not limited to the following:

- Minimal gaming despite large financial transactions with the entity;

- Structuring of transactions to stay at or slightly below reporting thresholds;
- A transaction that has no apparent business 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 negotiable instrument or wire transfer is presented for the benefit of multiple customers, or multiple customers engage in play on a single customer account;
- A customer refuses to provide required information or identifying information;
- A customer 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 customer;
- News articles or other media reports alleged acts of financial wrongdoing by the customer;
- A customer raises his or her financial transactions to levels well above the ordinary levels for that customer;
- A customer requests establishment of an account in the name other than the one by which the Company knows the customer;
- A customer 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 customer presents funds which the Company has a basis for suspecting to be the proceeds of illegal activity;
- A customer 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 customer, who is a big winner, enlists another individual (who is not a partner of the customer in the gaming activity) to withdraw a portion of the money won to avoid the filing of regulatory reports or other forms;
- A customer 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 customer exhibits unusual interest in the Company's reporting policies or inquiries about how the Company's business day is calculated.

4.6. 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 Money Laundering Reporting Officer (MLRO), 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 MLRO.

4.7. External Unusual Activity Reporting

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

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

Where the MLRO 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 MLRO 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 MLRO or a formally designated alternate;
- Include all relevant and available information required by the FIU.

The MLRO 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 customers suspected of terrorist financing and money laundering with other financial institutions so that these institutions can identify said customers when determining whether to engage in business with them.

6. Operating Procedures

6.1. Account Opening Procedures

Prospective customers must be introduced or referred to the Company's management by an existing customer or a known reliable source. Prospective customers 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 customers 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 customer 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 customer 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 customer 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 Company'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, and 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

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.

C. Drommond

Name: eMoore N.V.
Function: Director
Date: 20/02/2026

Executed by C. Drommond as Proxy Holder

