SailfourServices N.V.

Groot Kwartierweg 10 Livestrong Building, Willemstad, Curaçao

AML/CFT MANUAL

V. 2.0 - March 9, 2025

REVISION HISTORY

Version #	Date drafted	Author	Reviewer	Approved By	Comments
1.0	January 27,2025	iGaming Compliance Department	eMoore NV	Management	-
2.0	March 9, 2025	Igaming Compliance Department (Legal and Compliance)	eMoore NV	Management	

Table of Contents

Definitions and Abbreviations

Anti-money laundering (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.
Counter 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.
Counter proliferation financing (CPF)	Efforts focused on financing of the proliferation of weapons of mass destruction; the sale, transfer and export of nuclear, chemical or biological weapons and their means of delivery and related materials.
Counterparty	The business counterparty of the Company engaging with the Company for the provision of the Services offered by the Company onto its Website.
Cryptocurrency	Distributed, open-source, mathematically based peerto-peer virtual currencies that have no central administering authority, and no central monitoring or oversight. Examples include Bitcoin, Ethereum, Litecoin and Dogecoin.
Cryptocurrency transaction	The deposit and withdraw of cryptocurrencies into and out of a Player Account held by a Player.
The Company	Sailfour Services N.V., a limited liability company duly organized under Curaçao law registered with the Chamber of Commerce and Industry in Curaçao under number 165691.
Employee	Any person working for the Company.
FATF	Financial Action Task Force (www.fatf-gafi.org)
FIU	Financial Intelligence Unit of Curaçao (FIU)
KYC	Know Your Client, the mandatory process of identifying and verifying the identity of the Counterparty before

	entering into the business relationship and thereafter periodically over time.
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.
MLRO	Money Laundering Reporting Officer
Player	Individual who has registered on the Website of a Counterparty, for the purpose of making use of the Services offered on the Website and for which a Player Account has been opened.
Player Account	An account granted to an individual after registration on the Website of the Counterparty. The Player Account is created and issued by the Counterparty and is required for wagering with real money.
PEP	Politically Exposed Persons
Prohibited Jurisdictions	Jurisdictions prohibited under the Curaçao license conditions (Aruba, Belgium, Bonaire, Curacao, France, Netherlands, Saba, Sint Eustatius, Sint Maarten, USA) as well as jurisdictions restricted by decision of the Company's managing director when and where still applicable.
Service	the gaming and betting software developed and provided by the Company to its business partners.
Terms and Conditions	The terms and conditions for the use of the Services, as published on the Website of the Counterparty.
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 a Counterparty, for which the services of the Company is engaged.

1 AML/CFT Policy

1.1 Policy

Money Laundering, Terrorism Financing and the financing of proliferation of weapons of mass destruction are some of the 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 the true nature of the proceeds and/or the intended purpose. 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 through the use of criminal funds to fund gambling activities followed by the withdrawal of the funds on the player account thereby exchanging the criminally acquired funds for legitimate money.

ML, when not eliminated, can have far-reaching implications damaging the online gaming industry, and society as a whole.

Funds used for TF may not always be proceeds of criminal activities. Rather than an attempt to conceal the origin of the funds, as these may sometimes be from a lawful sources such as donations, it is an attempt to conceal the true purpose of the funds which is to support or conduct terrorist related activities. Terrorists regularly adapt how and where they raise and move funds and other assets in order to circumvent safeguards that jurisdictions have put in place to detect and disrupt this activity. Identifying, assessing and understanding TF risks is an essential part of dismantling and disrupting terrorist networks, as well as the effective implementation of the risk-based approach of CFT measures.

CPF 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 CPF measures, much like those related to CFT, involve identifying and assessing the risk of potential breaches or evasion of the targeted financial sanctions to proliferation financing and taking appropriate mitigating measures with the level of risks identified.

The Company takes AML/CFT/CPF seriously and has policies in place to ensure compliance with the regulations in the jurisdictions where we operate. The Company's procedures and internal controls are designed to ensure compliance with all applicable national and international regulations and will be reviewed and updated on a regular basis to ensure compliance with applicable legislation, regulation and changes in our business.

1.2 Objectives

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

a. ensure that statutory and regulatory obligations to prevent ML and TF are met, taking positive action to minimize risk of the Company's products and services being used for the purpose of ML or TF;
b. ensure that the Company does not engage with or continue established relationships with those whose conduct gives rise to suspicion of involvement with ML and/or TF;
c. terminate any relationships where the business-related activities gives the Company reasonable cause to believe or suspect involvement with illegal activities. Any such termination shall follow the reporting of the suspicion and thereafter shall be undertaken in conjunction with the relevant authorities and in accordance with the relevant regulations; and
d. comply with the Company's AML/CFT/CPF obligations based on national and international regulations.

1.3 Scope

This Policy applies to all persons working for the Company or on the Company's behalf in any capacity, including Employees, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external contractors, third-party representatives and business partners, sponsors, or any other person associated with the Company that falls within the scope of the Company's AML Policies.

This Policy defines procedures that will assist all persons working for the Company to comply with its legal obligations. Failure of an Employee to comply with the procedures defined within this Policy may lead to disciplinary action.

2 Regulatory Framework

2.1 National regulations

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 amongst others:

a. The National Ordinance on Money Laundering (P.B. 1993, no. 52);
b. 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 will 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.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;
d. The National Ordinance on Games of Chance (N.G. 2024, no. 157)
e. 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);
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); and
g. 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 or other criminal activities.

2.2 International regulations

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

On an international level, the FATF plays an important role in the combating of ML 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.

3 Procedures

To be compliant with the applicable rules, regulations and international standards, the Company has procedures in place to which it attains itself when providing Services to Counterparties. These procedures cover the following standards:

- Risk management
- Know Your Customer Procedure
- Reporting of unusual transactions
- Recordkeeping

4 Risk Management

4.1 Risk assessment

The possibility of online gaming being used by criminals to assist in ML and/or TF poses many risks for the Company, such as criminal and regulatory sanctions and/or reputational damage for the Company and/or its Employees. For this purpose, the Company must carefully identify its risks and manage them accordingly.

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

- Identifying, understand and assess the ML and TF risks relevant to the Company;
- designing and implementing appropriate policies, procedures and controls to manage and mitigate these risks;
- monitoring and improving the effective operation of these controls and identifying any weaknesses; and
- recording what has been done and why.

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

The risk assessment must identify and analyze the risks related to the following four key risk sources stemming from inherent vulnerabilities in the online gaming sector:

- Counterparties
- Product / service
- Geography

Counterparty Risk

The risk of ML/FT may vary in accordance with the Counterparty taking into account its identity and purpose of its business. The assessment of the risk posed by a Counterparty is generally based on the identity and integrity of the Counterparty, transactions related to the purpose of the business and the AML framework to which it adheres to.

Considering the AML risks involving Politically Exposed Persons (PEP), the Company has determined not to engage in any business relations with PEPs. PEPs are not considered to fall within the risk appetite of the Company.

The provisions as described further in the 'Know Your Client', specifically in the 'Transactions using Cryptocurrencies' sections below, must be noted.

Service Risk

Some gaming and betting software services and related transactions are inherently riskier than others and are therefore more attractive to criminals. These include types of games, betting products or services which are identified as being more vulnerable to criminal exploitation that allow Players to influence the outcome of a game, be it on his own or in collusion with others.

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 Counterparty. 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 following:

i. Prohibited Jurisdictions: these jurisdictions are prohibited under the Curaçao license conditions and/ or pursuant to a resolution of the Company's managing director;
ii. jurisdictions which are identified by FATF as high-risk jurisdictions subject to a call for action;
iii. jurisdictions under increased monitoring by FATF;
iv. countries which are identified by the European Union as high-risk countries;
v. countries which are identified by the United States as state sponsors of terrorism.

The Company must review its risk management processes on an on-going basis to ensure that it remains abreast of new risks. As a minimum, the risk assessment must be reviewed annually, or more frequently in the case of any important changes to products or technology, payment methods, customer type and other material changes.

The Company may decide not to proceed with further negotiations as soon as it considers the Counterparty to fall out of its risk appetite.

4.2 Risk Classification

Upon registration, the Company makes a risk classification of each Counterparty.

The Company maintains the following risk classification:

- Low risk
- Medium risk
- High risk

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

Type of Counterparties	**Monitoring frequency**
High risk Counterparties	3 months
Medium Risk Counterparties	6 months

Low Risk Counterparties	12 months

4.3 Money Laundering Reporting Officer (MLRO)

The Company has designated an MLRO who is in charge of the review of KYC information and the monitoring of transactions. The MLRO is in charge of the following:

i. ensure a proper review of the provided KYC documentation;
ii. conduct the necessary reviews as per the 'Know Your Customer Procedures' section below;
iii. provide initial and ongoing training to all relevant staff;
iv. reporting any unusual/suspicious transactions;
v. cooperate with all relevant administrative, enforcement and judicial authorities in their endeavor to prevent and detect criminal activity; and
vi. ensure that this policy is adhered to, reviewed and maintained regularly.

4.4 Transactions using Cryptocurrency

If the Counterparty offers the possibility of using cryptocurrency as a payment method, the following measures/conditions should be in place:

- the Counterparty shall conduct proper verification, including KYC and AML procedures, regarding its Players and persons who have applied to become a Player, including for those who will conduct their deposits using cryptocurrency;
- Cryptocurrency transactions are only possible if the initial deposit was made with a crypto currency. Following this transaction all transactions (deposits, wagers and payout) with the Player must be conducted using the same crypto currency as with the first deposit;
- The Counterparty will at no time sell/buy/exchange crypto currency with and/or to FIAT currency in relation to the Player transactions;
- Collect and verify proof of identity and proof of address as per its own AML/ CTF obligations and to make sure that the Player is over 18 years of age;
- Collection and storage of hardware KYC in all pathways from signup, login, deposits and withdrawals, including but not limited to IP address, mac address and browser information to ensure that all wagering, deposits and withdrawals are to/from the same Player (IP and computer);
- The Company will maintain proof of balance, to ensure Player's funds have been deposited;

- Maintain solvency to cover all bets and jackpots and that of the cryptocurrency.
- Ensure that the solvency funds is kept in a separate account and most recent proof thereof is maintained;
- The Counterparty will display the rate of exchange from crypto currencies to FIAT currency on the home page of the Website. In no way shall the Counterparty make exchanges between any cryptocurrency and any FIAT currency.
- The Company must include in their Terms and Conditions and highlights that cryptocurrency values can change dramatically depending on the market value.

It is important to note that due to the current anti-money-laundering regulations, a Player is to deposit money into its Player Account only in order to play and to use the services as provided by the Counterparty.

5 Know Your Customer Procedure

The Company is required to verify the identity of its Counterparties before or during the course of establishing a business relationship. The Company maintains a formal procedure in order to perform the KYC/due diligence checking. In most cases the Counterparty is a legal entity or legal arrangement. For identification and verification purposes of such Counterparties, the Company may request the following documents:

- a copy of the articles/ deed of incorporation or articles of association, or alternately a copy of the deed of trust if the Counterparty is a trust, or a copy of the partnership deed if the Counterparty is a partnership;
- an excerpt from the trade registry or a similar document evidencing the existence and Good Standing of the Counterparty;
- a list of directors; and
- a list of authorized signatories.

For the purpose of the identification of individuals acting on behalf of the Counterparty, or in case the Counterparty is an individual, the Company shall identify and verify individual’s full name and permanent residential address. For that purpose, the following documents are acceptable:

- a copy of current valid passport; and
- a copy of a proof of residence (utility bill or other document evidencing the individual’s address, like a bank or credit card statement)

5.1 Due Diligence

5.1.1 Standard Due Diligence

Standard Due Diligence is generally applied to low and medium risk Counterparties and is conducted in the following cases:

- before establishing the business relation; and
- anytime at the discretion of the Company.

In addition, the Company screens all prospect Counterparties against international sanctions lists.

5.1.2 Enhanced Due Diligence

If at the discretion of the Company, 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 take further actions amongst which the conduct of a thorough background check or the request of additional documentation.

If a (prospect) Counterparty fails to pass the background check, is discovered to be under active investigation or is suspected of ML/TF or other fraudulent activity, the Company will decide not to continue with further negotiations or terminate the business relation as this is considered to fall out of the risk appetite of the Company. The Company will further determine whether reporting to the relevant authorities is in place, in accordance with the applicable legislation.

6 Reporting of Unusual transactions

Any unusual transactions or circumstances for which the Company has not received sufficient explanation may give rise to its report to the FIU. 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. It is prohibited to inform a Counterparty or third parties of the reporting of or the intention to report an activity or transaction to the FIU.

7 Recordkeeping

The Company maintains a record of all relevant documentation on a separate database for at least five years after ending a business relationship. The Company is obliged to retain files in a way that enables investigating authorities to identify a satisfactory audit trail.

In specific circumstances, if ordered by rule of law and permitted by national law and the relevant authorities, the Company may provide copies of the records maintained.

8 Periodical review of AML/CFT policies

The AML/CFT policies of the Company are subject to a yearly review, comprising of a fair and unbiased appraisal of each of the required elements of this policy. The review may be conducted by an independent auditor or Employee or group of Employees, so long as the reviewer is not the MLRO and does not report directly to the MLRO.

9. Reporting to CGA

The Company shall provide information or documentation on their money laundering and terrorist financing policies and deterrence and detection procedures to the examiners of the GCB in preparation of or during an examination and upon GCB request during the year. The casino shall make the following items readily available:

- Its written and approved AML Compliance Program on money laundering, terrorist financing and financing of proliferation;
- Records of its Business Risk assessment;
- The name of each Compliance Officer responsible for the casino’s overall money laundering and terrorist financing policies and procedures and his/her designated job description;
- Records of reported unusual transactions;
- Records of unusual transactions which required closer investigations;
- Records of frozen accounts;
- Schedule of the training provided to the casino’s personnel regarding money laundering, terrorist financing and proliferation of weapons;
- The assessment report on the casino’s policies and procedures on money laundering, terrorist financing and financing of proliferation by the internal audit department or an external auditor;
- The customer’s files including customer risk assessment, CDD, customer acceptance and transaction information.

C Drommond

Signature: ___________________________

By: eMoore N.V. – Managing Director Date of Approval: 09/04/2025

eMoore N.V.

P.O. Box 422
Curaçao
Tel.: +59997471401