

ANTI-MONEY LAUNDERING MANUAL

Faro Entertainment N.V.

Approved by Global Related Services B.V., Corporate

Director by G. Hammoud

Date: May 29, 2025

Change History

Date	Ver.	Author	Summary Changes
01.04.2017	1.0	FARO ENTERTAINMENT N.V.	First Version
28.02.2020	2.0	FARO ENTERTAINMENT N.V.	New Version of ANTI-MONEY LAUNDERING MANUAL
06.04.2021	3.0.	FARO ENTERTAINMENT N.V.	New Version of ANTI-MONEY LAUNDERING MANUAL
11.01.2022	4.0	FARO ENTERTAINMENT N.V.	New Version of ANTI-MONEY LAUNDERING MANUAL
01.06.2022	4.1	FARO ENTERTAINMENT N.V.	Updated version of ANTI-MONEY LAUNDERING MANUAL
27-10-2023	4.2	FARO ENTERTAINMENT N.V.	Updated version of ANTI-MONEY LAUNDERING MANUAL
10-09-2024	4.3	FARO ENTERTAINMENT N.V.	Updated version of ANTI-MONEY LAUNDERING MANUAL
29-04-2025	4.4	FARO ENTERTAINMENT N.V.	Updated version of ANTI-MONEY LAUNDERING MANUAL

Note: This policy is subject to review at least once every 12 months or upon any material change in regulatory obligations, operational processes, or identified risks.

Next Scheduled Review: April 2026

Contact Information:

Name: Renos Yiangou

Position: Money Laundering Compliance Officer (MLCO)

Phone:

Email:

Table of Contents

1. PURPOSE	5
2. POLICY STATEMENT AND AUDIENCE	6
3. DEFINITIONS	7
4. INTERNAL CONTROLS, POLICIES AND PROCEDURES	8
5. RISK ASSESSMENT	9
6. CUSTOMER RISK GROUPS	9
7. IDENTIFICATION PROCEDURES	12
8. ENHANCED DUE DILIGENCE	14
9. POLITICALLY EXPOSED PERSONS AND SANCTIONS LISTS	16
10. ONGOING MONITORING	18
11. TRANSACTION MONITORING	18
12. RECORD KEEPING PROCEDURES	19
13. PROCEDURES FOR REPORTING	20
14. MONEY LAUNDERING COMPLIANCE OFFICER	20
15. MANAGEMENT OF FUNDS PROCEDURES	22
16. FRAUD MANAGEMENT PROCEDURES	22
17. ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM	23
18. PAYOUT MANAGEMENT	25
19. WHISTLEBLOWING PROCEDURE	27
20. STAFF CONTROL MEASURES	27
21. TRAINING	29
22. INTERNAL REVISION AND STAYING UP TO DATE	30
23. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE	31
APPENDIX 1 «UNUSUAL TRANSACTION REPORT»	33
APPENDIX 2 «COUNTRIES AND TERRITORIES EXCLUDED FOR REGISTRATION»	36

1. PURPOSE

1.1. FARO ENTERTAINMENT N.V., a limited liability company incorporated under the laws of Curaçao, with the company number 142227, having registered office at Kaya Richard J. Beaujon Z/N, Curaçao (hereinafter – the Company) has developed current AML Manual in accordance with the applicable legislation of the EU and Curaçao, reports of Financial Action Task Force and International standards of money laundering prevention, in particular (but not limited to):

- The Code of Criminal Law (Penal Code) (N.G. 2011, no 48);
- The National Ordinance on Identification of Clients when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- National Decree Penalties and Fines Reporting Unusual Transactions (N.G. 2021, no. 69), as amended by PB 2023, no. 6;
- National Decree supervisor identification when rendering services gaming sector (L.B. 28.01.2019, no. 19/0282);
- National Decree supervision unusual transactions gaming sector (L.B. 28.01.2019, no. 19/0283);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- National Decree for general measures, of the 10th July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015, no. 30);

- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Ordinance extension of validity sanction decrees (N.G. 2018, no. 34);
- National Decree Prohibition to Import, Export and Transit of Venezuelan Gold (N.G. 2019, no. 82);
- National Ordinance on the Obligation to Report Cross-Border Money Transportation (N.G. 2002, no. 74), as amended by (N.G. 2014, no. 90);
- National Ordinance on Offshore Games of Hazard (PB 1993, no. 63);
- Curacao Gaming Control Board, Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025.

The Company checks for amendments to all Decrees and Regulations on a regular basis and updates the policies and procedures accordingly to meet any such changes. Besides these regulatory authorities, the Company also continually observes relevant international standards such as the recommendations of the Financial Action Task Force on Money Laundering ('FATF'), the Caribbean Financial Action Taskforce (CFATF) and the Guidelines and instructions of the European Commission as well as the six Directives of the European Union on AML and CFT.

2. POLICY STATEMENT AND AUDIENCE

- 2.1. The Money Laundering Regulations place obligations on the Company and its employees (incl. individual contractors) with respect to suspected money laundering, the key points being:
- The reporting and detection of suspected money laundering.
 - Officers must be vigilant for the signs of money laundering.
 - Any employee who suspects money laundering activity must report this promptly to the Company's Money Laundering Reporting Officer (see reporting form for completion by the officer unusual of activity).
 - No payment to the Company will be accepted in cash..
- 2.2. Where the Company is carrying out certain regulated activities during day-to-day business then the customer due diligence procedure must be followed.
- 2.3. The Money Laundering Regulations are complex and detailed and should there be any doubt about the policy requirements, please request further information from the Money Laundering Compliance Officer 'MLCO' or line management.
- 2.4. The fight against crime demands that criminals are prevented from legitimizing the

proceeds of their crime by the process of «money laundering or terrorist financing». It is a process which can involve many outside the more obvious targets of banks and other financial institutions.

2.5. The launderer or terrorist financier often seeks to involve many other often unwitting accomplices, such as:

- stockbrokers and securities houses;
- insurance companies and insurance brokers;
- financial intermediaries;
- surveyors and estate agents;
- gaming activities;
- company formation agents;
- dealers in precious metals and bullions;
- antique dealers, car dealers and others selling high value commodities and luxury goods.

2.6. The vast majority of criminal dealings are done in cash. Criminals need ways to dispose of the cash and have it re-appeared as part of their wealth with as little chance as possible of it being tracked back to the cash element.

3. DEFINITIONS

3.1. Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities.

3.2. Criminals misuse the financial system by hiding the true origin of the funds, gained from illegal activities.

3.3. If undertaken successfully, it also allows them to maintain control over those proceeds and ultimately to provide legitimate cover for their source of funds. Their «dirty» funds come to appear «clean».

3.4. In the gaming sector, money laundering methods often involve using criminal proceeds to fund gambling activities, placing large bets with minimal risk, or cashing out after limited play to present the funds as legitimate winnings, or utilizing online gambling platforms to transfer illicit funds across jurisdictions.

3.5. Despite the variety of methods employed, the laundering process is typically accomplished in three stages. These three stages may comprise numerous transactions by the launderers that could raise suspicions of underlying criminal activity:

- Placement – the physical disposal/deposit of the initial proceeds derived from illegal

activity.

- Layering – separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity. Such transactions are often channeled via shell companies or companies with nominee shareholders and/or nominee directors.
- Integration – the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

3.6. Terrorism financing refers to providing financial resources to individuals or groups involved in terrorist activities. This includes gathering, transferring, and using funds to support terrorism, either directly or indirectly. These funds can come from both legal sources, like donations and business earnings, and illegal activities, such as drug trafficking, smuggling, and fraud.

3.7. The main goal of terrorism financing is to aid in the planning, preparation, and execution of terrorist acts, which can severely impact national and global security.

3.8. Online gaming companies are particularly at risk of being exploited by terrorists for money laundering or covert fund transfers due to the sector's anonymity and high transaction volumes.

3.9. Proliferation financing involves providing financial resources or services to aid in the development, acquisition, or spread of weapons of mass destruction (WMD) and their delivery systems. This includes funding the purchase of materials, technology, and expertise needed for the creation and deployment of nuclear, chemical, and biological weapons.

3.10. Proliferation financing is a significant threat to global security and stability, as it facilitates the distribution of WMDs to both state and non-state actors who might use them for harmful purposes.

4. INTERNAL CONTROLS, POLICIES AND PROCEDURES

4.1. The Company is required to establish and maintain policies, procedures, and controls to prevent money laundering or terrorist financing, and to ensure the reporting of any that may be known or suspected.

4.2. Key elements of a sound Anti-Money Laundering program, required by law, are:

- Customer Risk Assessment.
- Identifying clients and due diligence procedures (Identification Procedures).
- Record-keeping procedures in relation to client's identity and their transactions.
- Procedures of internal reporting to a Money Laundering Compliance Officer appointed to

receive and consider information that gives rise to knowledge or suspicion that a client is engaged in money laundering.

- Through examination of each transaction, which by its nature may be considered to be particularly vulnerable to be associated with money laundering offences and in particular unusual patterns of transactions which are carried out with no apparent economic or visible lawful purpose (e.g., transfer of funds between members).
- Measures to make employees aware of all the procedures systems and controls in place.

4.3. Unusual transactions should be reported where there is suspicion of money laundering, funding of terrorism or that the funds being used on the Company's website are the proceeds of criminal activity.

5. RISK ASSESSMENT

5.1. The development and implementation of an effective AML Manual is based on a risk assessment. For this reason, the Company is required to conduct an AML/CFT risk assessment of its business, customers, products and the geographic location in which it operates, in accordance with a standard risk assessment methodology. In identifying potential risks and threats across the industry the following categories have been considered:

- Customer risk - specific categories of customers and the resulting business relationships.
- Payment risk - payment methods offered by operators and the degree to which their specific characteristics are vulnerable to ML/TF threats.
- Geographical risk - the risks posed by geographical factors.
- Product risk - products offered and the degree to which their specific characteristics may be attractive for the purpose of money laundering or financing terrorism.
- Employee risk - the risks posed by the employees of every operator.

6. CUSTOMER RISK GROUPS

6.1. Every new customer is placed in one of the 4 main Risk groups (Very High, High, Medium, Low) based on his Risk level score (between 0 and 100). The Risk level score is calculated by the Company's Anti-Fraud team upon the revision of the newly registered accounts. The score (also known as "Customer score card") is a sum of multiple checks on KYC Data to validate the identity of the individual (who they are, where they live, their age, how to contact them) and additional Fraud Management Data to assess the value of potential risk of the

individual (all relevant information that is needed to analyze the risk associated to the used IP address and e-mail address, their physical location and the ID of the device being used).

6.2. At a minimum, the following factors are considered during the risk assessment process:

- Customer Risk: Includes the customer's background, occupation, and transaction patterns. High risk customers, such as Politically Exposed Persons (PEPs) and those from high-risk jurisdictions are given special attention.
- Product/Service Risk: Evaluates the risk associated with the products and services offered. High-value transactions, anonymous transactions, and new or complex products are scrutinized more closely.
- Geographic Risk: Considers the risk based on the geographic location of the customer and the transaction. Countries with weak AML regulations or high levels of corruption are considered higher risk.
- Delivery Channel (Interface) Risk: Assesses the risk associated with the methods used to deliver products and services. Non-face-to-face transactions and digital channels may pose higher risks.

6.3 The Anti-Fraud team further monitors Company's customers upon financial activities or gaming behavior and can assign the customer to a different Risk group at a later stage. A combination of certain parameters, such as personal information, used payment methods, significant change of betting behavior or unusual activity, detection of multi-accounting, dormant accounts and source of customer's funds is what defines the Risk groups.

A. Very high-risk customers (Risk level score: 75 - 100)

Company's Anti-Fraud team is trained to evaluate and tag customers according to the volume of their financial transactions and casino/sport betting gaming activity. In addition, if the team identifies a customer who carries a very high potential for money laundering, the case is forwarded to the MLCO for further investigation. Very high-risk customers are subject to Enhanced Due Diligence (EDD). The monitoring of identified very high behavior is a key factor in preventing ML/TF activity.

- Customers who trigger the AML alert (transactions equal or higher than the amount of 2000 EUR are present).
- Customers who are trying to register from/log in from FATF listed Countries marked as High-Risk Counties.
- Customers with extensive (covering or affecting a large number of payment methods,

consecutive high amount deposits in short period of time, wagering high amounts on minor/young leagues [e.g. may have internal information about the outcome of the event]) financial and/or betting activity.

- Customers who send unclear/incomplete/corrupted documents on their Customer Due Diligence.
- Customers who were found to be using VPN/Proxy servers.

B. High risk customers (Risk level score: 50 - 75)

Similar to the very high risk customers group, the high risk customers are missing one (or more) of the key factors in their overall profile, however their residence (part of the UN/EU Sanctioned and FATF listed countries) and/or behavior still rise concerns for a potential money- laundering fraud or possible terrorist financing. High-risk customers are subject to Enhanced Due Diligence.

C. Medium risk customers (Risk level score: 25 - 50)

The customer's risk level may increase or decrease, depending on his behavior over time. A medium risk customer is defined as such when a number of the risk factors which are mentioned above are present but one or a few of the essential ones is/are missing (country risk, payment risk, betting risk).

- Customers who are not conspicuously changing their betting patterns (significantly increasing their stakes in minor sports events, placing bets on opposite outcomes, or constantly placing repetitive bets).
- Customers who are exclusively using the Payment method chosen upon their initial deposit.

D. Low risk customers (Risk level score: under 25)

In order to be considered as part of the low-risk group, the customer must have sent clear and up-to-date identification verification documents which after in-depth checks are recognized by the Anti-Fraud team as legitimate. Furthermore his/her financial transactions should include a single payment method with consistent deposit and withdrawal amounts and the customer's country of registration/login should not be included in the UN/EU Sanctioned and FATF listed Countries.

- Customers who are not recognized by the Company's dedicated internal system software for using VPN/Proxy servers and/or don't share the same or similar IP addresses with

other customers.

- Customers who follow strictly Company's "Terms of Use" and don't make attempts to manipulate or abuse the rules of the Company in any way.

7. IDENTIFICATION PROCEDURES

7.1. The Law requires all persons carrying on financial business to maintain client identification procedures. The Company applies general (standard) customer due diligence (hereinafter – CDD) measures to the customers at the registration stage. The CDD process consists of:

- Identifying the player and verifying that customer's identity using reliable, independent source documents, data or information;
- Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, such that the casino is satisfied that it knows who the beneficial owner is. For legal persons and legal arrangements this should include understanding the ownership and control structure of the customer;
- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the casino's knowledge of the player, its business and risk profile, including, where necessary, the source of funds.

7.2. To access the games, Faro Entertainment N.V. requires the prospective player to enter all mandatory information requested on the registration form on the website, in particular: name and surname, address and contact details, valid email address, passport number, relevant payment information (including credit card number, expiry date), all of which the client warrants to be true and correct. Faro Entertainment N.V. reserves the right to close an account should any information prove to be false or misleading as a result of verification mechanisms employed by the Company. For payouts the user has to upload his passport and a utility bill and after review and approval of these documents, the payout will be done.

7.3. CDD measures are implemented when customers conduct financial transactions of Naf. 4,000 or more (or its equivalent in another currency), engage in occasional transactions exceeding this amount, there is suspicion of money laundering or terrorist financing, or the casino questions

the accuracy or sufficiency of previously obtained customer identification data. If the Naf. 4,000 threshold is met and CDD is incomplete, the customer will be prevented from depositing or withdrawing funds. If the customer does not provide the required documentation when needed, the account will be closed after 30 days, and a report of unusual activity will be filed if there is a reasonable suspicion of money laundering or terrorist financing.

7.4. CDD process is vital for the prevention of money laundering. If a client has established a business relationship under a false identity, he/she may be doing so for the purpose of defrauding our company itself (i.e., climbs the ranking ladder with minimum cost) or merely to ensure that he/she cannot be traced or linked to the proceeds of the crime that our company is used to launder. CDD procedures describe the process by which the identity, background, and other aspects of the source of wealth of a customer is being checked.

7.5. Appropriate documents for verifying the identity of customer include, but are not limited to, the following:

- High resolution photocopies of relevant pages of client's passport
- High resolution photocopies of relevant pages of client's ID card

Both above need to clearly state the following: Full names (personal and surname), date of birth, place of birth, nationality, current address, date of issue, expiration date, country, identification number, signature.

To verify the address of the customer the Company requires one of the following to be provided, in the same correct name of the customer:

- High resolution photocopy of a utility bill (fixed-line phone, water, electricity) issued within the last 3 months
- High resolution photocopy of a tax or rates bill from a local authority
- High resolution photocopy of a bank statement (for a current account, deposit account or credit card account) or High resolution photo copy of a bank reference letter.

7.6. Customer details are reviewed by the team to ensure their accuracy and in certain cases further proof of address and identity might be requested, particularly in cases where the customer becomes active. Certain customers are highlighted automatically as higher risk customers and can by default not make deposits automatically into the system. Such customers are assigned a higher risk level based on a number of parameters, including but not restricted to: country of residence, country of issuing credit card, IP log, number of transactions within a defined period etc.

The behavior of clients is also taken into account to control and manage profitability, charge backs and fraud, problem behavior including compulsive gambling. This is to a large

extent managed manually by the management and team but the use of the payment processing back office is also used to perform various checks and procedures.

- 7.7. Customers depositing an amount in a defined period that is above a limit set by the management will be required to provide additional details (income statement) to avoid account closure. Faro Entertainment N.V. also carries out regular checks to all depositing clients such as, log analysis, contact with customers, monitoring of unusual activity using administration system as well as those management systems provided by our payment providers.
- 7.8. All records shall be preserved in accordance with Paragraph 12 of this AML manual.

8. ENHANCED DUE DILIGENCE

- 8.1. The Company applies enhanced customer due diligence measures (hereinafter – EDD) and enhanced ongoing monitoring, in addition to the required customer due diligence measures, within the scope of the risk analysis adopted. EDD is applied to mitigate the money laundering or terrorist financing risks arising in the following cases:

- in any case, identified by the Company or in the information provided by the authorities to the Company as one where there is a high risk of money laundering or terrorist financing;
- if the customer is a citizen of a high-risk country;
- if the customer makes use of products or performs transactions that may favor anonymity;
- If the Company has doubts as to whether the information collected regarding the identity of the customer is correct or not (or no longer) accurate;
- if the Company has determined that a customer or potential customer is a PEP, or a family member or known close associate of a PEP;
- in any case where the Company discovers that a customer has provided false or stolen identification documentation or information and the Company proposes to continue to deal with the customer;
- in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose,
- if the payment of a customer's winnings is made to a different payment account of the customer than to the account from which the customer makes the wagers
- When new products and business practices are introduced, including new delivery

mechanisms and the use of new technologies for both new and existing products

- in any other case which, by its nature, can present a higher risk of money laundering or terrorist financing.

8.2. In cases where there is a higher risk, establishment of the business relationship or continuation of the business relationship (if the higher risk only arose later or was only recognized later) only with the consent of a member of the Company's management level. If a customer has been deemed to be a high-risk or becomes one at any stage, the Company undertakes the EDD, comprising of (depending on the case):

- undertaking Re-verification of identity (repeated CDD).
- Establishing how the customer acquired his wealth to be satisfied that it is legitimate:
- salary income or company profit (Certified Pay slip / Certified employer letter / audited accounts if self-employed)
- sale or liquidation of financial instruments (Certified shares/investments sale contracts or statements/ accountant letter)
- sale of property (Certified copy of the contract of sale or letter from a solicitor or estate agent)
- inheritance (Certified copy of will including the value of heritage)
- sale of the company (Certified contracts, media articles, certified letter from accountant or solicitor).
- Establishing the source of the customer's funds to be satisfied that they do not constitute the proceeds from crime.
- Ensure that deposits originate from payment methods and do not allow anonymity by requesting copies of bank statements or account statements.
- Where possible, contacting the payment method provider to confirm their confidence in the good standing of the mutual customer.
- In the case of a PEP, gain a better understanding of the customer's reputation and/or role in public life and assessing how this affects the level of risk associated with the business relationship
- Undertaking increased continuous monitoring of the business relationship.
- The unusual transaction must be investigated, and the business relationship underlying the transaction shall be monitored to assess the risk of money laundering and terrorist financing.

- 8.3. Meaning of Source of Funds. The Source of Funds refers to the origin of the particular funds being used to deposit on the Company's website. This is not simply verifying which bank or financial institution the customer may have received the funds from. The information obtained should be substantive, relevant and establish the fund's origin and the method/circumstances under which the funds were acquired.
- 8.4. Meaning of Source of Wealth. The Source of Wealth refers to the origin of the entire body of wealth (i.e., total assets) of the client. The information that the Company obtains should indicate the volume of wealth the client would reasonably be expected to have and provide a picture of how it was acquired. dered as part of the customer`s risk assessment. A customer`s PEP status will also be checked at significant events in the customer`s relationship with the company, such as

9. POLITICALLY EXPOSED PERSONS AND SANCTIONS LISTS

- 9.1. The Company manually runs the data of newly depositing customers across industry recognised and global third-party Financial Sanctions, PEP and adverse media screening databases and those issued by the United Nations and the European Union. Further risk-based checks may be made using closed and open sources and if any adverse information is found, this will be considered as part of the customer`s risk assessment. A customer`s PEP status will also be checked at significant events in the customer`s relationship with the company, such as when obliged to carry out Customer Due Diligence, large withdrawals, and any other identified potentially unusual activity.
- 9.2. Sanctions screening shall be performed on customers at the moment of account opening, when a customer request to withdraw funds from their accounts and in instances whereby the legislative framework governing sanctions applicable to Curaçao is subject to amendments or expansions.
- 9.3. The Company shall immediately and without prior notice freeze the funds or assets of designated sanctioned persons and entities in accordance with United Nations Security Council resolutions and the European Union`s Common Foreign and Security Policy. In such cases, a report shall be filed with the FIU and the Company shall immediately proceed to freezing the resources of the customer concerned. When and if a match is confirmed by the supervisory organization, the Company shall terminate the provision of services to the customer and shall inform the supervisory organization on the type and amount of the frozen resources and on the

actions that are being undertaken to implement the sanctions order or sanction decree on the basis of which the resources have been frozen.

9.4. Any new or existing customer found on the Sanctions database, or a PEP or relative of such will have their account rejected, when still in the registration stage, or closed, when the active customer's status has changed.

9.5. In case of identifying a PEP, responsible staff will send a report to ML officer within 30 days from the date on which a customer was considered a PEP, who in turn will send a report to the MLCO.

9.6. The MLCO will investigate each case to identify positive or false-positive PEP alert. The Company has a right to request additional documents from the customer for this purpose within the investigation.

9.7. If the PEP alert is true-positive, the MLCO will decide to reject registration or close the account and inform the senior management about the decision taken.

9.8. Politically Exposed Person means any person who has been entrusted with a high- ranking prominent public function at the international, European, or national level or who is or has been entrusted with a public position of comparable political importance below the national level. In particular, politically exposed persons are:

- heads of state, heads of government, ministers, members of the European Commission, deputy ministers and assistant ministers,
- members of parliament and members of similar legislative organs,
- members of the governing bodies of political parties,
- members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are usually not subject to further appeal,
- members of the boards of courts of audit,
- members of the boards of central banks,
- ambassadors, chargés d'affaires and defence attachés,
- members of the administrative, management or supervisory bodies of state-owned enterprises,
- directors, deputy directors, members of the board or other managers with a comparable function in an international or European intergovernmental organization.

Family member of PEP means a close relative, in particular

- the spouse or civil partner,
- a child and the child's spouse or civil partner and

- both parents.

10. ONGOING MONITORING

10.1. The general due diligence duties include the ongoing monitoring of the business relationship. This includes:

- Obtaining fresh identification when existing documents have expired. (This can be done on a risk-sensitive basis.)
- Questioning the data and information the Company have whenever inconsistencies are noticed.
- general review and update from time to time, on a risk sensitive basis.
- checking if transactions match with the documents and information available at the Company about the customer and the origin, customer's assets
- updating the respective documents, data, or information at appropriate intervals.

10.2. When the Company conducts ongoing transaction monitoring and notices that a customer's transactions deviate from expected patterns, it shall investigate this unusual activity and, if necessary, determine the source of the funds used. Additionally, the Company shall revise the risk profile of the player. The extent of ongoing monitoring will depend on the customer's risk profile.

11. TRANSACTION MONITORING

11.1. The Company retain a record of every transaction undertaken for a customer to establish the financial/behaviour profile and provide a satisfactory audit trail. The transaction monitoring is carried out through Coverly solution, by which the Company identifies the following unusual activity (including, but not limited to):

- a customer opening an account and registering several different cards and making transfers between them,
- a customer depositing large sums, then places minimal stake bets, then withdrawing all their funds,
- a customer depositing large amounts and repeatedly losing large amounts as if the loss is of no consequence,
- money is deposited by a customer or held over a period and withdrawn by the customer without being used for gambling,
- a customer tries to register several gaming accounts.

12. RECORD KEEPING PROCEDURES

- 12.1. The Law requires, firms to retain records concerning client identification and details of transactions for use as evidence in any possible investigation into money laundering. This is an essential constituent of the audit trail procedures that the Law seeks to establish.
- 12.2. The Company keeps all the documents and data collected or obtained within the scope of the due diligence, including:
- all data and information used to identify and verify customers (including type and number of the document, issuing authority, etc.)
 - all records (receipts) relating to transactions, i.e., winnings paid out or refunds to customer accounts,
 - all documents and records used for the preparation of the risk analysis, the risk analysis itself, including the results of the risk assessment, as well as the documentation on the appropriateness of the measures taken based on these results,
 - the results of the internal investigations
 - documents collected within the scope of business partners due diligence
 - documents collected from the employees within the scope of the due diligence
 - documents regarding AML trainings (training materials, examination results, etc.)
- 12.3. The Company also keeps all documents created and processed in connection with a suspicion of money laundering or terrorist financing, including:
- all related internal and external correspondence,
 - file and interview notes,
 - the results of internal investigations and the measures taken, that can explain why the money laundering officer concluded and initiated the actions taken.
- 12.4. The retention period is ten years and starts with the end of the calendar year in which the business relationship ends and in all other cases with the end of the calendar year in which the respective information was ascertained. Applicable legislation may provide for a more extended retention period.
- 12.5. The Company destroys all the documents and data collected after retention period expiration unless other recordkeeping or retention obligations apply, but not later than after 10 years.

13. PROCEDURES FOR REPORTING

- 13.1. All employees have a duty to report unusual and suspicious transactions. If an employee has any suspicion about a customer's behaviour or transaction, it must be reported to the MLCO immediately. All employees are expected to report unusual and suspicious transactions to the MLCO.
- 13.2. The employee should still submit the report, even if their superiors are not in agreement. It will then be up to the MLCO to determine if the information available can be considered as sufficient for a UTR to be made to the FIU.
- 13.3. Internal UTRs must be submitted to the MLCO email - aml@faroentinc.com. The following information should be included:
- account details
 - detailed reason for suspicion
- 13.4. The MLCO will:
- acknowledge receipt of the report and review and investigate further as required
 - make an assessment based upon all the information and decide whether the matter needs to be reported to law enforcement and/or the FIU.
 - if it does, also submit a UTR to the FIU, if it doesn't the MLCO will determine whether it does require to be reported to the FIU based on the indicators provided for the sector.
 - make a record and inform senior management about the decision taken
- 13.5. Where the report is based on the objective indicators, as outlined by pertinent Curacao legislation, such reports shall be submitted to the FIU within 48 hours of the transaction taking place.
- 13.6. Where the report is based on the subjective indicators, as outlined by pertinent Curacao legislation, such reports shall follow the timeline below:
- Internal UTR must be submitted to the MLCO within 24 hours of the transaction taking place
 - MLCO must make a determination as to the reportability of the transactions within 10 working days
 - If the MLCO determines that the transaction and/or behaviour is indicative of ML/TF, the MLCO must submit the report to the FIU within 48 hours of making that determination.

14. MONEY LAUNDERING COMPLIANCE OFFICER

- 14.1. Employees should report their knowledge or suspicion of transaction or activities

involving money laundering to the Money Laundering Compliance Officer (MLCO). If there is a suspicion of a transaction or activity it should be reported and documented as per Appendix 1 «Unusual Transaction Report» UTR).

14.2. Next to any internal reports received, the MLCO is always responsible for reporting to the Financial Intelligence Unit FIU, in all cases where a transaction meets the indicators for providers of internet gaming and gambling as mentioned in the Ministerial Decree on the indicators for Unusual Transactions.

14.3. The MLCO has the responsibility to receive and process UTRs. Once an MLCO receives an UTR, s/he carries out the following:

- Record the UTR and assess the information provided by the reporter;
- Maintain a record of the UTR having been received and maintain an updated timeline of events during its processing stages;
- Assesses whether the reported activity constitutes potential ML/FT; and
- Decide whether there is scope to escalate the UTR externally to the FIU. If not, reasons for not escalating are recorded.

14.4. In the case of a decision to escalate the UTR externally:

- Escalate UTR to FIU by documenting and submitting the UTR in the FIU GoAML portal; and
- Advice (senior) management on execution or delay of the transaction and even possible termination of the relationship with the customer.
- Document in detail the reasoning for all decisions taken and advice given in order to support the course of action.

14.5. In respect of the person who initially escalated the UTR:

- Confirm receipt of UTR to sender;
- Provide an internal UTR reference to be quoted should further updates in relation to the UTR need to be raised;
- Remind the person escalating the UTR of the obligations not to tip off the customer nor to divulge information about the escalation of the UTR to third persons both internally and externally; and
- If a transaction was flagged during a processing stage, decide whether transaction is to be put on hold or processed. Due consideration must be exercised to assess whether external escalation is being considered to FIU and whether holding the transaction at this stage

may raise suspicions on the customer's end which could jeopardize investigations by the FIU and relevant authorities.

15. MANAGEMENT OF FUNDS PROCEDURES

- 15.1. The purpose of the management of funds procedures is to outline the process, actions and responsibilities in handling the funds of the company.
- 15.2. Employees of the Faro Entertainment N.V. must carefully read, obey and comply with the below contents/guidelines.
- 15.3. This procedure must be read in conjunction with anti-money laundering procedure and fraud management procedures.
- 15.4. To request a payout on winnings in Faro Entertainment N.V. the user must request the withdrawal by clicking on «Payout». The user needs to indicate the preferred payment method.
- 15.5. The system only allows payment methods which also have been used to make a deposit in the past. Furthermore, a credit card refund can only be made to the same credit card the original deposit has been made with.
- 15.6. When the user has selected the chosen payment method and entered the desired amount, the system checks:
 - if the payment method is allowed for that particular user;
 - if any outstanding wagering multipliers have been fulfilled.
- 15.7. In case of error, the corresponding error message is displayed to the user. Alternatively, the input is processed. The desired payout amount is deducted from the player's balance.
- 15.8. If everything is ok, the payout is processed and removed from the «open payout» queue. The user is informed via e-mail or internal messaging channel that the payout has been processed.
- 15.9. Any unusual behavior in relation to payouts must be handled according to the AML Policy.

16. FRAUD MANAGEMENT PROCEDURES

- 16.1. The purpose of the fraud management procedures is to outline the process, actions and responsibilities in the event of a fraud and/or unusual transaction occurring within the company.
- 16.2. Employees of the Faro Entertainment N.V. must carefully read, obey and comply with the below contents/guidelines, with respect to fraud management, KYC policies and anti-money laundering procedures.
- 16.3. This procedure must be read in conjunction with anti-money laundering procedure and management of funds procedures.

- 16.4. Employees of Faro Entertainment N.V. will be properly screened prior to employment with the Company. Prospective employees will be required to submit police conduct certificates, bank references and passport/ID information approval for employment with the Company from the Authority. Once the documents are provided, these should be checked by Human Resources team for authenticity and any doubts should be escalated to concerned Manager. Additionally, these are to be screened using public sources (e.g., internet search engines & media) to identify any further public information about the candidates which may be beneficial or detrimental for the expected role.
- 16.5. The Company will appoint a Fraud Control Manager charged with the supervision of the Company's workforce. He will engage in a process of checks and balances of members of the staff on a regular basis. Any detection of fraud will be immediately addressed by the Company internally, or if the seriousness of the fraud warrants such, the Company will inform the competent authorities to provide the Company with specialist assistance on the matter.
- 16.6. Fraud Control Manager shall also be in charge of fraud screening of players and player transactions. The Company shall deploy fraud Management and Control software which will bring to the attention of the Fraud Control Manager irregularities in players and player transactions. The Fraud Control Manager shall be responsible for escalating and dealing with any unusual transaction.

17. ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM

- 17.1. The purpose of AML procedures of Faro Entertainment N.V. is not to allow the Company, its resources, its business, its services, or its employees to be used or involved in a money-laundering activity or scheme, to detect and report any incident, including unusual transactions, to relevant competent authorities in accordance with the applicable Anti-Money Laundering Regulations, to preserve all relevant information that is in Company's possession that may be required by the relevant authorities investigating an unusual activity, and to cooperate with the said authorities as may be necessary.
- 17.2. The Company maintains a comprehensive, risk-based AML compliance program designed to mitigate risks in line with applicable laws, regulations and international standards. The company has implemented the following measures:
- Correct KYC Procedures;
 - Monitoring and assessment of player's risk indicators and payment risk indicators;
 - Mitigation of risks by implementing appropriate payout policies;

- Designation of an MLCO;
- Ensuring employees are aware of the risks, procedures and their obligations with respect of AML reporting;
- Procedures to block accounts based on suspicion of money laundering or terrorist financing;
- Periodic re-assessment of the situation and adjustment of policies as may be required to ensure that they are adequate at any time. Such assessment must be appropriate and must be reviewed as necessary in the light of any changes of circumstances, including the introduction of new products or technology, new methods of payment by customers, changes in the customer demographic or any other material changes, and in any event reviewed at least annually. The MLCO is responsible for the monitoring, update and management of compliance with, and the internal communication of, AML policies and procedures.

17.3. To make sure there is no illegal activity taking place, the following procedure are set in motion:

- Identification and verification procedures are enforced.
- Customers are allowed to cash out only to the same Payment method / account they had previously used to deposit. In case it is not technically possible, the customer is being further investigated (direct call, request for extra documents, etc.) until he/she proves that the second Payment method of choice is secure and belongs to him/her.
- All transactions are carried from customers' accounts to the Company's accounts and vice versa. There is neither money lending, nor offsetting balances allowed between customers.
- Only one account per person/family/household address is allowed, preventing customers from trying to manipulate the systems and using multiple payment suppliers for money laundering.

17.4. Red flags are not intended to automatically result in filing a UTR with the FIU, however, are merely indicators that should lead the Company to question the customer's behaviour. If there is no reasonable explanation for the red flags, then an internal report must be made to the MLCO. The following is a list of possible red flags which should be considered:

- Customer does not cooperate in the carrying out of CDD.
- Customer attempts to register more than one account on a site.
- Customer makes small wagers, even though the amounts deposited are significant,

followed by a request to withdraw well in excess of any winnings.

- Customer makes frequent deposits and withdrawal requests without any reasonable explanation.
- Noticeable changes in the gaming patterns of a customer, such as when the customer carries out transactions that are significantly larger in volume when compared to the transactions he normally carries out.
- Customer enquiries about the possibility of moving funds between accounts belonging to the same gaming group.
- Customer carries out transactions which seem to be disproportionate when seen in the context of what is known about the Customer's wealth, income or financial situation.
- Customer seeks to transfer funds to a bank account held in the name of a third party.
- Customer requests a withdrawal to an account he never deposited with.
- a customer opening an account and registering several different cards and making transfers between them,
- a customer depositing large sums, then places minimal bets, then withdrawing all their funds,
- a customer depositing large amounts and repeatedly losing large amounts as if the loss is of no consequence.

18. PAYOUT MANAGEMENT

- 18.1. This document describes the Faro Entertainment N.V. Payout management procedures.
- 18.2. In order to request a payout, a member must first have KYC approval. Otherwise, they cannot request for a payout.
- 18.3. If the member has KYC approval, they can request a payout by clicking on «Payout».
- 18.4. The system checks if the member has enough funds available in their account.
- 18.5. The system checks to see if the member used that payment method as a deposit method in the past and if payment requisites of deposit transactions match with those of withdrawal requests.
- 18.6. There is a minimum limit of at least 20 EUR and a maximum limit of 100,000 EUR for a payout. If the member enters less than 20 EUR or more than 100,000 EUR to be paid out, they receive an error message and they must enter an acceptable figure between 20 EUR and 100,000 EUR the amount entered by the member is deducted from the account.
- 18.7. For all payout requests, the following checks are performed:
 - KYC documents;

- How the winnings were acquired;
- Payouts and payout history;
- History of account;
- Deposit history.

- 18.8. Know Your Customer documents are official documents that can verify a person's identity and address of residence. Documents accepted to verify a person's identity are: a government issued valid ID, passport or driver's license.
- 18.9. Documents accepted to verify a person's residential address are: a utility bill (water, electricity, telephone or internet), a bank statement from a recognized Bank or a Residence Registration Document from their local authority office. To accept proof of address documents from a member, the document should not be more than 3 months old.
- 18.10. Funds that come from direct deposits, transfers, redeemed gift certificates or suspicious gameplay, are not payable and a follow up message is sent to the member via Admin. In case of suspicious gameplay, the account is suspended, pending a full investigation of game logs and account history.
- 18.11. Past payouts are also checked every time a member asks for a new payout. If the member has successfully received payouts to the same bank account in the past, the payout is processed. if the member enters a new bank account, the payout is declined and we ask for a bank reference letter or a bank statement, to have proof of bank account ownership.
- 18.12. If the member is trying to use a bank account that has been used by another member in the past, the payout is declined and the member is informed that we need a proof that the bank account is of joint ownership or to send us a bank reference letter or bank statement for their own bank account. They are then informed that all payouts will be processed to their own bank account.
- 18.13. Additionally, checks are done to ensure that the banking information received is valid (Valid IBAN and BIC/Swift codes). In case an IBAN or BIC contains spaces, special characters or lower-case letters, the payout is declined and we ask that they enter their information in the proper form before requesting a new payout. In cases of invalid BICs and IBANs we ask for a bank reference letter (when the case does not involve a digit or a letter mistype).
- 18.14. History of account is also checked for important notes left from support, regarding any unusual activity or behavior. If there is such a note, the payout is declined and the customer is contacted.
- 18.15. Player deposits are always checked daily to make sure that all credits in account were actually received in the back end of the payment method. When the member requests a payout,

we double-check that there were no issues with deposits credited to the account in the past.

- 18.16. If after all the checks the payout is approved, we submit it to the 2nd list of payouts, from which we create a bank batch file every day and submit it to the bank to process. The payout is removed from the 1st queue (open) queue and the funds are removed from the member's account. If some of the payouts in the Bank Batch file cannot be processed (due to invalid IBANs and BICs or in cases where the BIC submitted does not match to the corresponding IBAN) we are informed by the bank. The payout is placed on hold and we inform the member to send us the banking information we need. When the information is received, payouts that were previously placed on hold are manually processed through the online banking system, while the banking details in the member's account are updated to the correct ones.

19. WHISTLEBLOWING PROCEDURE

- 19.1. This document describes the Faro Entertainment N.V. Whistleblowing procedure.
- 19.2. The Whistleblowing procedure is independent of the Unusual Transaction Report as per Appendix 1 «Unusual Transaction Report» (UTR). However, the Whistleblowing procedure may be used if the employee feels that his/her UTR reports have been disregarded or mishandled.
- 19.3. For all the below, communication may be done in either anonymous or identified escalations, depending on the employee's preference. It is important however, especially if the employee decides to remain anonymous, that all relevant information (evidence, dates, names of involved people) is provided when escalating such an instance. **ANONYMOUS REPORT:** any Whistleblowing Report that comes from an individual whose personal details are unknown or not clearly identifiable. You may report anonymously by email using your personal email or specially created email address to make sure that your personal details remain unknown to us.
- 19.4. Where an employee believes that fellow employees, management or top management is not applying AML policies and procedures appropriately, or individual customer risks are not treated appropriately and there is a potential or real risk of the company being highly exposed to Money Laundering, the employee may alert any of the following, depending on the level of risk:
- MLCO: The company's MLCO via email at aml@faroentinc.com;
 - Board of Directors: Send email to the company directors on ceo@faroentinc.com. These will review and take action as appropriate.

20. STAFF CONTROL MEASURES

- 20.1. The Company has a number of internal controls and general procedures which are used

on a day-to-day basis in respect of managing and running the daily operations of the business for the purpose of money laundering and terrorist financing prevention.

20.2. Specific actions shall require the approval or authorization of senior management or MLCO personnel before being carried out by employees. Therefore, the Company will implement a system of access levels throughout the Company, whereby access to data and other inside information owned by the Company shall only be granted to selected employees. The Company shall determine such access and the extent to which it is given according to the role and position of the relevant employee case by case. At all times, no employee shall have any access that is in excess of his needs to perform the work expected of him through his role and position.

20.3. The Company will allocate duties to be performed by employees in such a manner that no one employee shall have complete and sole control over an entire process or an entire area. This approach prevents fraudulent behaviour from being undertaken by employees due to the level of power they are granted over a particular section of the operation. In cases where it would not be beneficial for the Company to have a specific duty or task split between different employees, the Company will ensure that the employee who is given full control over such process or area shall be adequately supervised in proportion with the fraud risk level that such process or area may pose.

20.4. Prior to engaging employees, the Company will carry out relevant integrity checks, in-line with their position, responsibilities and access levels. The Company will not employ any persons who are not deemed to be fit and proper.

For this purpose, the Company may request the following documents (in each case with due regard to data protection):

- a valid original identity document,
- CV,
- any other documents as the Company deems necessary to request.

20.5. Once a person is employed, screening shall still be carried out on an ongoing basis as required. All Company's employees must guarantee that they observe the provisions of the applicable legislation and the associated due diligence obligations, report facts relevant to money laundering, and do not themselves participate actively or passively in dubious transactions.

20.6. For this purpose, senior management will regularly carry out checks on employees or whenever the Company feels the need to perform such inspections. In particular, such inspections shall be carried out when suspicion arises concerning the behaviour of specific employees. The Company may carry out these checks through surprise spot checks or other procedures that will

enable such personnel to verify whether employees comply with the policies and procedures.

20.7. The frequency and extent of screening that shall be carried out shall be proportionate to the risk level posed by the employee. The risk level will be determined case by case depending on employee's position (e.g., head of dept, senior, mid), the scope of duties and obligations, etc.

20.8. The Company must check all the employees (who work for one year) at least once a year. The Company will use an employee performance sheet for this purpose.

21. TRAINING

21.1. The Company give training to all staff directly or indirectly through a service provider upon joining the Company and after that annually. Relevant training materials are prepared for all teams based on the company policies which have been compiled according to the applicable legislation requirements and guidelines. Training will be conducted as follows:

- Training material based on the finalized and approved policies the Company has, in the form of documents and presentations.
- Training will be provided to existing management and staff in a class setting.
- Training will also be included in the induction of all new staff.
- Training will be followed up with a questionnaire to test everyone's understanding.
- Should the Company find that some issues are not clear we will repeat the training focusing on the issues that were not understood.
- Regular refresher training will be given, which will include any updates and will focus on any shortfalls that arose during the previous period.
- Any update in policy will be communicated in a group email and through ad-hoc training and added to periodic training updates and material.

21.2. Staff training is focus on ensuring awareness of:

- The provisions of the money laundering and terrorist financing requirements,
- Their personal obligations under the money laundering and terrorist financing requirements,
- Any applicable internal reporting procedures,
- The Company's policies and procedures to prevent money laundering and the financing of terrorism,
- The Company's participant and business participant identification, verification, recordkeeping, and other procedures to prevent money laundering and the financing of

terrorism,

- The recognition and handling of unusual transactions,
- Their personal liability for failure to report information or suspicions in accordance with the money laundering and terrorist financing requirements and the license holder's internal procedures; and
- New developments, including information on current techniques, methods and trends in money laundering and the financing of terrorism.
- Data protection regulations.

21.3. Induction training sessions will be conducted for all employees and will include fraud prevention, detection, and ancillary matters, as required by their role. Refresher training will also be provided, both on a regular basis and as needed, to keep employees up to date and informed of the Company's policies and procedures and any changes or improvements made.

21.4. The MLCO keeps records of training delivered, showing what training has been provided, when and by whom, and the next training date. In case of any changes to the Company's policies and procedures or applicable legislation, all staff will get the relevant training.

22. INTERNAL REVISION AND STAYING UP TO DATE

22.1. The Company has compiled its policies and procedures according to the requirements and guidance of legislation specified in subsection 1.1 of this Manual. The Company is aware that the requirements and guidance and external fraud trends can and will change and that the Company must keep up its policies and procedures and procedures to date. The Company may use third-party service providers to internal revise all documents and processes for compliance with the relevant legislation and regulations. Therefore, the measures will be implemented to ensure the Company is kept up to date:

- Key personnel will subscribe to any mailing lists offered by the regulator and will join relevant forums.

22.2. In the case of an update, the following steps will be taken, as necessary:

- Update company policy documentation and training material.
- Inform all relevant staff by email regarding the updates, meet with relevant team managers, and ensure they update their teams appropriately.

- Update email communication templates and chat canned responses.
- Update website policies, maintaining a version number and “last update” date.
- Update the Terms and Conditions, maintaining a version number and ‘last update’ date.

Any consequential update to the Terms and Conditions will trigger a pop-up notification to customers on their next login where they will need to accept and agree to the new version before proceeding.

23. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

The Company is committed to full compliance with all applicable anti-money laundering (AML) and counter-terrorist financing (CTF) laws and regulations of Curaçao, including the National Ordinance on the Identification of Clients when Rendering Services (NOIS) and the National Ordinance on the Reporting of Unusual Transactions (NORUT).

All employees and relevant officers must adhere strictly to the obligations set forth under these laws, including but not limited to: conducting proper customer due diligence, monitoring transactions, reporting unusual transactions to the FIU Curaçao without delay, maintaining the confidentiality of reporting activities, and cooperating as defined under the legislation.

Violations and Corresponding Penalties

According to the applicable regulatory framework, the following acts constitute violations that may result in supervisory or criminal sanctions:

- Failure to Report Unusual Transactions (Article 11 NOIS): Not reporting actual or intended unusual transactions to the FIU Curaçao.
- Failure to Provide Requested Information (Article 12(2) NOIS): Not submitting required data or documents within the timeframes established by law.
- Improper Reporting Procedures (Article 13 NOIS): Not following prescribed procedures for submitting reports or supplying information.
- Breach of Confidentiality (Article 20(2) NOIS): Using or disclosing sensitive information in a manner not authorized by the legislation.
- Failure to Comply with Supervisory Guidelines (Article 22h(3) NOIS): Disregarding mandatory instructions issued by the supervisory authority.

Sanctions and Enforcement Measures

Pursuant to the NORUT and NOIS:

- Periodic Penalty Payments (Article 22a(2) NORUT): A maximum penalty may be imposed for failure to comply or to comply in time with legally imposed obligations.

- Administrative Fines (Article 22b(2) NORUT): May be levied per day for continued non-compliance.

Criminal Penalties:

- Intentional violations: Considered a criminal offense punishable by imprisonment of up to four years, or an administrative fine, or both.
- Non-intentional violations: Considered a minor offense, punishable by detention up to one year, or a fine, or both.

Internal Disciplinary Measures

In addition to legal and regulatory sanctions, the Company may impose internal disciplinary action on employees or officers found to be in violation of the AML/CTF policy, including but not limited to:

- Written warnings,
- Suspension,
- Termination of employment or engagement.

Any instance of non-compliance is treated with the utmost seriousness and may also trigger a formal internal investigation and audit review.

The Company continuously monitors regulatory developments and updates its policies and procedures accordingly to ensure full alignment with the supervisory framework set by the FIU Curaçao, Curaçao Gaming Control Board (GCB), and other relevant authorities.

APPENDIX 1

«UNUSUAL TRANSACTION REPORT»

1. GENERAL INFORMATION

- 1.1. Surname
Name
Username
Email address
Telephone number
Request amount
Amount paid
Fee EUR
Ticket number
Request date
Processed date

2. BANKING INFORMATION

- 2.1. IBAN
BIC
Bank name
Has the member requested a Payout in the past? If yes, enter previous banking details:
IBAN
BIC
Bank Name
- 2.2. If banking details match, please proceed to 3.1 of the Identification Procedures.
- 2.3. If banking details do not match, please complete 3.1 and 3.2 below.
- 2.4. Other Checks:
Made a call to the member for further info to the payout
Inform the member that the payout is not possible, by email
Do the banking details match to those of another member? If yes, clarify
Surname
Name
Username

3. IDENTITY PROCEDURES

3.1. KYC check

Passport/ID

Valid passport

Bill/Address

If the passport expired, please ask for a new one

3.2. Due diligence check

Passport or ID to be certified by a public notary

Police conduct certificate

Bank reference letter

Note: Use your judgment for the due diligence check, to see if you need to request all or one of the above. Keep in mind the following:

- Look at the amount requested
- Rational of the Transaction
- Pattern of the Transactions
- If member gave us different banking details, then with his previous Payouts, request a Letter from the Bank confirming all his details.

4. INTERNAL TRANSFERS

4.1. Received funds from other members?

Note: Internal transfer of funds between members, for Payouts, is strictly prohibited. Treat the account as unusual and double check the «Identity Procedures». If yes, inform the member that it is not possible to make the payout and to manually have the funds transferred back to his account.

5. OTHER SECURITY CHECKS

5.1. Is the transaction normal for the member?

Can the withdrawal be explained?

Checked for similar accounts?

Do we have a letter of confirmation from the bank for shared banking?

Is the bank in the same country as the member?

Was the transaction fee deducted from the account?

Were the funds deducted for withdrawal?

If there is any contradiction, please specify and state your actions.

Other comments or remarks you want to add for the Payout.

6. ACCOUNT CONTROL

6.1. Personal account

If there is anything wrong, please provide a short description

Amount withdrawn

Withdrawal date

Signature

Message(s) from the member

Date of message

Report completed by: _____ Date: _____

Checked by MLCO: _____ Date: _____

APPENDIX 2

«COUNTRIES AND TERRITORIES EXCLUDED FOR REGISTRATION»

Below a compiled list of banned countries, however, it is not exhaustive and might also include other countries that may have been banned due to various reasons, e.g., change in FATF recommendations, countries banned by license agreements, countries with other AML / CFT deficiencies etc.

1. Afghanistan
2. American Samoa
3. Aruba
4. Australia
5. Austria
6. Belize
7. Belgium
8. Bonaire
9. Bosnia and Herzegovina
10. Burma/Myanmar
11. Burundi
12. Central African Republic
13. Curaçao
14. Democratic Republic of the Congo
15. Egypt
16. Eritrea
17. Estonia
18. France
19. French Guyana
20. Germany

21. Greece
22. Greenland
23. Guadeloupe
24. Guam
25. Holy See (Vatican City)
26. Italy
27. Iran (human rights)
28. Iran (nuclear proliferation)
29. Iraq
30. ISIL and Al-Qaida
31. Ivory Coast
32. Lebanon
33. Libya
34. Lithuania
35. Kuwait
36. Malaysia
37. Marshall Islands
38. Martinique (.FR)
39. Maldives
40. Mali
41. Netherlands
42. North Korea (Democratic People's Republic of Korea)
43. Occupied Palestinian Territory
44. Poland
45. Puerto Rico
46. Qatar
47. Reunion
48. Republic of Guinea
49. Republic of Guinea-Bissau
50. Russian Federation
51. Saba
52. Saint Barthelemy
53. Saint Martin

- 54. Saint Pierre and Miquelon
- 55. Singapore
- 56. Spain
- 57. South Africa
- 58. Somalia
- 59. South Sudan
- 60. St. Eustatius
- 61. Sudan
- 62. Sweden
- 63. Syria
- 64. Tunisia
- 65. Turkey
- 66. USA
- 67. US Minor Outlying Islands
- 68. US Virgin Islands
- 69. Venezuela
- 70. Yemen
- 71. Zimbabwe