

Last updated: 18th of December, 2025

ANTI-MONEY LAUNDERING AND TERRORIST FINACING: GUIDELINES FOR THE ONLINE GAMBLING INDUSTRY

A2F B.V.

Policy Version: 1.2 (Effective: 18 of December, 2025)

Legal Entity Name	A2F B.V.
Legal Status	Limited Liability Company (registered under the laws of Curaçao)
Company Number	151745
Registered Address	Abraham Mendez Chumaceiro Boulevard 50, Willemstad, Curaçao
License Number (GCB)	OGL/2024/298/0109
Operational Websites	apostasbf.com / aposrasnow.com / bet-bra.com / betuppro.com / bolsadeaposta.com / captainpunt.com / drinbet.com / fulltbet.com / peakodds.com / punterplay.com / sharpbet.com / superodds88.com / tradeball.com / oddjusta.com
Responsible Office	Compliance Department
Next Review Date	December 2026

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

Contents	Pages
1. Purpose	4
1.1. Policy Statement	4
1.2. Regulatory context	5
1.3. Legal basis	7
1.4. Definitions	7
1.5. Industry responsibility	8
2. Money Laundering	8
2.1. What is money laundering?	8
2.2. Stages of money laundering	9
3. Terrorist Financing	9
3.1. What is terrorist financing?	9
4. Internal Controls, Policies and Procedures	10
4.1. Systems and Procedures	10
5. Responsibilities of the Board of Directors	11
6. Compliance Officer	12
6.1. Appointment of Compliance Officer	12
6.2. Reporting Procedures	12
6.3. Internal Reporting procedures – Reporting to FIU (MOT)	12
6.4. Preparation of client list	13
6.5. Detection, recording and evaluation of risks and updating of procedures	13
6.6. Training	13
6.7. Reporting	13
7. Application of appropriate measures and procedures on a Risk Based Approach	14
7.1. Application of measures and procedures on a risk-based approach	14
7.2. Identification, recording and evaluation of risks	14
8. Design and implementation of measures and procedures to manage and mitigate the risks	15
9. Customer due diligence	15
9.1. Description and Analysis	15
9.2. Casinos	15
9.3. DNFBPs supervised by the FIU (MOT) and GCB	16
10. A2F B.V. client's identification procedures	16
10.1. Individuals	17
10.2. Enhanced CDD for high-risk categories of customers	23
10.3. Risk-based approach	25
13.3.1. Risk classification	26

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

Contents	Pages
11. Monitoring and improving the measures and procedures	27
11.1. Effective Transaction Monitoring	28
11.2. A system of independent testing of the policies and procedures	28
12. Recognition, documentation, and reporting of unusual transactions	29
12.1. Recognition of unusual transactions	29
12.2. Wire transfer	29
12.2.1. The documentation of unusual transactions	30
12.2.2. Reporting of unusual transactions	30
12.2.3. Internal reporting	30
12.2.4. External reporting	30
13. Record keeping	31
13.1. Time period of keeping documents / data	32
13.2. Format of records	32
13.3. Certification and language of documents	32
13.4. Description and analysis	32
14. Employees' obligations, education and training	32
15. Offenses and Sanctions in the NORUT and the NOIS	33
15.1. Penalties related to the NORUT and the NOIS	34
15.2. Administrative fines related to the NORUT and the NOIS	34
15.3. Referral for criminal investigation in accordance with the NORUT/NOIS	35
Appendix 1: Glossary/Definitions	36
Appendix 2: Internal Reports for Money Laundering	38
Appendix 3: Source of Funds Declaration Form	42

1. Purpose

The present document forms the procedures manual for the prevention of money laundering and terrorist financing of A2F B.V., a limited liability company registered under the laws of Curacao with Reg. No. 151745, having its registered address at Abraham Mendez Chumaceiro Boulevard 50, Willemstad, Curaçao.

The guidelines are meant to complement legal and regulatory requirements, irrespective of the jurisdiction where A2F B.V. is licensed. The manual is intended to help the management team and the employees of the Firm to follow procedures that they can be confident are broadly in line with industry best practice.

The aim of the company and regulator in this sector should be to build a proportionate and risk-based AML & CTF regime. Any model adopted should be continually reviewed to ensure that it continues to cover all elements of possible risk. This methodology in turn ensures the best use of resources, value for money, and highlights the factors that represent the greater risk.

A2F B.V. acknowledges the importance of following both the letter and spirit of such law and all relevant directions, recommendations and instructions and wishes not to be used by any of its clients for the purpose of carrying out money laundering or terrorist financing activities.

The manual is intended to provide guidance to the management team and the employees of the operator of the procedures to be followed so as to prevent and fight potential money laundering or terrorist financing activities.

This manual contains comprehensive due diligence procedures in accordance with the Law that shall be followed by the operator, its management team and its employees, in relation to the identification of clients, record-keeping and recognition and reporting of suspicious transactions.

1.1. *Policy Statement*

The legalization of proceeds of criminal activities or “Money Laundering” (hereinafter “ML”) refers to all activities intended to conceal the illegal source of funds. The financing of terrorism (hereinafter “FT”) refers to activities intended to channel funds to third parties for terrorist purposes. This policy also covers the combating of the Financing of Proliferation of weapons of mass destruction (hereinafter “FP”). The solvency and the reputation of the operator, as well as the reliability of the financial system in general, may suffer greatly as a result of the efforts made by criminals to conceal the source of the proceeds of criminal activities or to channel funds to terrorist activities.

Identifying the risks arising from ML, FT and FP activities and their potential consequences, as well as the importance of combating financial crime, and taking also into account the provisions of the

recommendations of the Financial Action Task Force (F.A.T.F.) and the specific Curaçao legal framework in force, including the National Ordinance on the Reporting of Unusual Transactions (NORUT), the National Ordinance on Identification when rendering Services (NOIS), and the Sanctions National Ordinance, the operator has introduced and applied an Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation Policy. This policy has been approved by the Board of Directors of the operator.

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

More specifically:

With respect to procedures, these:

- Are adapted to the nature of the business activities of the operator and comply with the local regulatory framework in force.
- Are assessed at least annually by an independent audit function and must be revised when deficiencies are identified or when the need arises to make adjustments.
- Are approved by the Board of Directors of the operator and must be communicated to the Company's Staff, to whom duties and responsibilities are clearly allocated

With respect to IT systems, these:

- Are capable of providing timely and reliable information for controlling the clientele and the transactions, on the basis of the lists of persons or entities subject to sanctions, as such lists are issued by the various Authorities.
- Allow continuous monitoring and detection of transactions or activities which may be associated with ML or FT, using specific parameters (indicative typology of transactions, customer's financial/transactional profile, expected account activity etc.).
- The operator has appointed an AML/CFT Officer and an alternate thereof. The AML/CFT Officer is responsible for ensuring the proper and adequate implementation of the AML/CFT Policy and for ensuring the company's full compliance with Targeted Financial Sanctions (TFS).

The key components of the AML/CFT Policy are the following:

- Responsibilities of the AML/CFT Officer
- Customer Acceptance and Cooperation Policy
- Continuous Monitoring of Accounts and Transactions
- Reporting of Unusual/Suspicious Transactions
- Monitoring Operator's Compliance level to the Regulatory Framework

1.2. Regulatory context

Curacao is committed to the fight against money laundering and terrorist financing. Because of this commitment, and its membership to both the Financial Action Task Force on Money Laundering (FATF) and the Caribbean Financial Action Task Force (CFATF), Curacao has a comprehensive framework to prevent and combat money laundering and terrorist financing. In addition, Curacao regularly attends both the FATF and CFATF meetings.

The main laws or executive decrees relating to money laundering and terrorist financing

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

(where applicable as amended) are:

- a) The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- b) The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G. 2009, no. 65 (N.G. 2010, no. 41) (NORUT);
- c) The National Decree containing general measures on the execution of articles 22a, paragraph 2, and 22b, paragraph 2, of the National Ordinance on the Reporting of Unusual Transactions (National Decree on Penalties and Administrative Fines for Reporters of Unusual Transactions) (N.G. 2010, no. 71);
- d) The National Ordinance on Identification of Clients when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2009, no. 66 (N.G. 2010, no. 40) (NOIS);
- 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) Ministerial Decree with general operation of May 21, 2010, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Decree Indicators Unusual Transactions) (N.G. 2010, no. 27);
- g) Ministerial Decree with general operations of March 15, 2010, implementing the National Ordinance on Identification of Clients when Rendering Services (N.G. 2010, no. 11);
- h) Ministerial Decree with general operation of March 15, 2010 for the execution of the NORUT (N.G. 2010, no. 10);
- h) 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);
- i) National Ordinance on the Obligation to report Cross-border Money Transportation (N.G. 2002, no. 74);
- j) National Decree providing for general measures, of 8th August 2011, for the implementation of articles 1, first paragraph, subsection b, under 16°, 6, subsection d, under 12° and 11, second paragraph, of the National Ordinance on the Identification of Customers when Providing Services (National Decree designating services, data and supervisors under the National Ordinance on the Identification of Customers when Providing Services); and
- k) National Decree providing for general measures, of 8th August 2011, for the implementation of articles 1, first paragraph, subsection a, under 16°, and 22h, second paragraph, of the National Ordinance on the Reporting of Unusual Transactions (National Decree designating services, data and supervisors under National Ordinance on the Reporting of Unusual Transactions).

These laws and decrees serve as the basis for further actions by the financial sector of Curaçao to detect and deter money laundering and terrorist financing.

The Provisions and Guidelines contribute to the adequate implementation by all supervised Entities of:

- relevant provisions of all the above-mentioned Ordinances and decrees.

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

- sound internal policies and procedures to detect and deter money laundering and terrorist financing.

The objective of the above-mentioned policies and procedures is to minimize the possibility that supervised entities become involved in money laundering and terrorist financing activities, and thus minimize the risks that their reputation and that of the financial sector of Curaçao will be adversely affected.

Furthermore, the latest laws and decrees represent the implementation of the original 40 FATF recommendations to combat money laundering issued in 1990 and lastly revised in 2003. After the September 11 terrorist attacks, the FATF extended its mandate to combat the financing of terrorism. In October 2001, the FATF issued 8 special recommendations on terrorist financing. In 2004 it issued the 9th special recommendation on terrorist financing. These Provisions and Guidelines on the Detection and Deterrence of Money Laundering and Terrorist Financing issued by the Central Bank aim to achieve compliance with the FATF 40 recommendations of 2003 and the nine special recommendations on terrorist financing.

1.3. Legal basis

The gaming industry operating in and from Curaçao is held to compliance with the primary national legislations:

- National Ordinance on identification when rendering services (NOIS) (also known as Landsverordening identificatie bij dienstverlening (LID), PB 2017, no. 92);
- National Ordinance on the reporting of unusual transactions (NORUT) (also known as Landsverordening melding ongebruikelijke transacties (LMOT), PB 2017, no. 99);
- The Sanctions National Ordinance (Landsverordening inzake sancties);
- The Kingdom Sanction Act (Rijkswet op de sancties).

With the publication of the National Decree supervisor identification when rendering services gaming sector (Landsbesluit toezichthouder identificatie bij dienstverlening kansspelsector, LB van 28 januari 2019, no. 19/0282) and the National Decree supervisor unusual transactions gaming sector (Landsbesluit toezichthouder ongebruikelijke transacties kansspelsector, LB van 28 januari 2019, no. 19/0283), the Curaçao Gaming Control Board (GCB) is tasked with the AML/CFT supervision of the gaming sector operating in and from Curaçao.

1.4. Definitions

This guideline is designed to be familiar with the concept of money laundering and the methods most commonly used by money launderers, but for the sake of clarity money laundering can be described as the process(s) by which criminals conceal or attempt to conceal the origin of the proceeds of their or others' criminal activities. The process of layering money may take place over several stages with gaming being just one part of that process. The aim, once money has been laundered, is that it can then appear to be legitimate. However, the operator should check whether their country's definition of money laundering also includes illegal activities that are far more subtle

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

and difficult to detect. Our obligation is to check how their countries have enacted the issue of predicate offences.

A more recent development and a sub-category has been money laundering to support terrorist financing. The fight against that particular strand of money laundering is commonly known as Counter Terrorism Financing (CTF). This is another crucial area to consider because terrorists and their supporters may commit crimes in order to finance acts of terrorism. However, terrorist financing can also occur when money earned legitimately is provided to terrorist groups for an illegitimate purpose.

1.5. *Industry responsibility*

Money laundering and terrorist financing are serious international issues and it is important that such criminal activities are identified and prevented by all available means. The CFATF has identified betting/casinos as one of many industries that may be attractive to those who wish to commit crime, conceal the profits of their crime or fund terrorist activity. By extension the online gambling industry therefore has a duty to detect and prevent money laundering and the funding of terrorism wherever possible.

2. Money Laundering

2.1. *What is money laundering?*

Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If undertaken successfully, it also allows them to maintain control over those proceeds and to ultimately provide a legitimate cover for their source of funds. In other words, their “dirty” funds come to appear “clean”.

All money laundering has three common factors:

1. criminals need to conceal the true ownership and origin of the money;
2. they need to control the money; and
3. they need to change the form of the money.

A simple transaction may be just one part of a sophisticated web of complex transactions illustrated below. Nevertheless, the earliest key stage for the detection of money laundering operations is where the cash first enters the financial system.

The operator has the obligation to identify their (prospective) clients/customers, including, where applicable, the (ultimate) beneficiaries of their prospective clients/customers, before rendering them their services. The operator must maintain an information program to inform those clients of the objectives of the relevant anti-money laundering legislation and inherent requirements for the gaming industry.

The internal procedures of an operator must clearly indicate for which services clients or their representatives must identify themselves and which identification documents are acceptable.

The allowed client identification documents and the nature of the transaction are prescribed in the NOIS 14. The required information must be regularly updated and adequately documented. Operator should have and follow clear standards on what records must be kept on the aforementioned areas, including individual transactions, account files and business

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

correspondence and on their retention period for current as well as terminated business relationships. An important objective for the operator is to be able to retrieve this information, without any undue delay. Hence, the supervisory authority requires the operator to implement a checklist containing identification and/or transaction information, and to maintain a centralized record keeping system to retain copies. Operator should ensure that the identification documents are valid at all times. Reference is in this respect also made to article 3, paragraph 3 of the NOIS.

2.2. Stages of money laundering

There are three stages of money laundering during which there may be numerous transactions made by launderers that could alert supervised entities to criminal activity.

I. Placement:

During this first stage of the money laundering process, illegal monies are introduced into the financial system e.g. through deposits in a bank account. Illegal proceeds are easier to detect at the placement stage, when the physical currency enters the financial system.

II. Layering:

Illicit proceeds are separated from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.

III. Integration:

This stage provides apparent legitimacy to criminally derived wealth or income. 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 to be normal business funds.

3. Terrorist Financing

3.1. What is terrorist financing?

A supervised entity that carries out a transaction, knowing that the funds or property involved are owned or controlled by terrorists or terrorist organizations, or that the transaction is linked to, or likely to be used in, terrorist activities, is committing a criminal offence. Such an offence may exist regardless of whether the assets involved in the transaction were the proceeds of criminal activities or were derived from lawful activities but intended for use in support of terrorism.

Terrorist financing is the financial support, in any form, of terrorism or of those who encourage, plan or engage in terrorism. It generally falls into two broad categories:

- Funding the direct costs associated with undertaking terrorist acts
- Funding required maintaining a terrorist network, organization or cell.

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

Terrorist financing varies in scale and sophistication, ranging from organized fundraising by domestic cells which are part of a larger, organized international network, to funds raised by small, loosely organized and self-directed groups. Smaller groups may raise funds for their own domestic use, as well as provide funding to overseas groups with whom they sympathize.

3.2. What is financing of Proliferation of weapons of mass destruction (FP)?

Financial assistance related to the manufacture, acquisition, possession, development, export, trans-shipment or use of nuclear, chemical or biological weapons.

4. Internal Controls, Policies and Procedures

4.1. Systems and Procedures

The operator shall comply with sanctions imposed by the United Nations, European Union, United Kingdom, and United States (OFAC). A system of regular updates will be maintained to monitor these sanctions lists, ensuring real-time integration into the compliance framework. The operator shall leverage AML software to screen clients, transactions, and counterparties against these lists, and any potential matches will be escalated to the Compliance Officer for immediate review.

Client funds must be maintained in segregated accounts separate from the operator's operational accounts. These accounts will be reconciled daily, with oversight by the Compliance Officer to ensure adherence to segregation requirements.

In order to enable the detection and prevention of money laundering and the financing of terrorism, the company must have adequate and appropriate systems in place which cover the following:

- **Customer identification and due diligence** – know the customer and his business. Due diligence is carried out at the start and on a regular basis throughout the business relationship with the customer. Additional due diligence is required in the event that the client carries out transactions for NAF 5,000 or more whether the transaction is carried out in a single operation or in several operations which appear to be linked and in the event of suspicion of money laundering or terrorist financing regardless of the amount of the transaction, and when there are doubts about the veracity or adequacy of previous customer identification data. Customer identification procedures and customer due diligence measures comprise:

- a. identifying the customer and verifying their identity on the basis of documents, data or information obtained from a reliable and independent source;
- b. identifying the beneficial owner and taking risk-based and adequate measures to verify the identity on the basis of documents, data or information obtained from a reliable and independent source so that the person carrying on in financial or other business knows who the beneficial owner is; as regards legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the customer;
- c. obtaining information on the purpose and intended nature of the business relationship;
- d. conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

conducted are consistent with the information and data in the possession of the person engaged in financial or other business in relation to the customer, the business and risk profile, including if necessary, the source of funds and ensuring that the documents, data or information held are kept up to date.

The extent of these measures and identification procedures may be determined on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction. The persons must be able to demonstrate to the competent supervisory authorities that the extent of the measures is

appropriate in view of the risks of the use of their services for the purposes of money laundering and terrorist financing.

For the purposes of identification procedures and customer due diligence requirements, proof of identity is satisfactory if it is reasonably possible to establish that the customer is the person he claims to be; and the person who examines evidence is satisfied, in accordance with the procedures followed under this Law, that the customer is actually the person he claims to be.

- **Record-keeping** – client and transaction information must be maintained for a period of five years following the end of a relationship with a customer.

- **Internal reporting and reporting** to Ministerial Decree Indicators Unusual Transactions (*The indicators which apply are laid down in a joint ministerial decree of the Minister of Finance and the Minister of Justice, which decree is based on Article 10 of the NORUT.*) – The appointed money laundering compliance officer needs to report any suspicious transactions both internally and to FIU (MOT).

- **Internal control, risk assessment and risk management.**

- **Transaction examination** – transactions that are considered to be particularly vulnerable to money laundering and terrorist financing, complex, unusually large transactions, and transactions with unusual patterns must be examined closely.

- **Informing employees** – employees must be informed of systems, procedures, and legal requirements in relation to combating money laundering and terrorist financing.

- **Training** – ongoing relevant training to employees.

4.2. Employee Screening and Vetting Program

The Company shall maintain a mandatory, risk-based Employee Screening and Vetting Program. This program is designed to ensure that all personnel adhere to high ethical and professional standards, particularly those in roles that are critical to the AML/CFT framework.

- **Scope:** Screening procedures shall be applied to all employees, directors, and officers, with enhanced scrutiny focused on individuals in high-risk functions, including Compliance, Management, Payments, Customer Service, and Finance.
- **Procedure:** Screening shall involve verification of professional and personal integrity, criminal background checks (where legally permissible), and verification of qualifications relevant to the role.
- **Ongoing Monitoring:** Vetting is an ongoing process. Staff in high-risk roles shall be re-screened periodically, and any staff changes or adverse information must be promptly reported to the Board of Directors and the Compliance Officer for review.

5. Responsibilities of the Board of Directors

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

The Board of Directors is responsible for:

- I. the determination, recording and approval of the general policy principles of the Company, in relation to the prevention of money laundering and terrorist financing and its communication to the Compliance Officer;
- II. the appointment of a Compliance Officer and, where necessary, assistant Compliance Officers;
- III. the determination of the duties and responsibilities of the compliance and assistant Compliance Officers;
- IV. the approval of the clients' acceptance policy;
- V. the approval of the risk management and procedures manual;
- VI. the communication of the risk management and procedures manual to all employees;
- VII. the application of all requirements of NORUT/NOIS;
- VIII. the introduction of appropriate, effective and sufficient systems and controls;
- IX. the day to day compliance of money laundering and terrorist financing obligations within the areas of the Firm;
- X. the provision to the Compliance Officer with prompt advice of unusual/suspicious transactions and other matters of significance;
- XI. the provision to the Compliance Officer with complete and timely access to all data and information concerning clients' identity, transactions' documents and other relevant files and information maintained by the Firm so as to fulfil their function effectively;
- XII. the provision to the Compliance Officer with the appropriate resources to fulfil their function effectively;
- XIII. for ensuring that the Compliance Officer has complete autonomy in the suspicious transaction reporting (STR) evaluation process and unfettered access to information necessary to carry out that process;
- XIV. for ensuring that all employees are aware of the person who has been assigned the duties of the Compliance Officer, as well as their assistants;
- XV. the establishment of a clear and quick reporting chain of suspicious transactions to the Compliance Officer.
- XVI. The AML policy shall be reviewed and signed annually by the Money Laundering Reporting Officer (MLRO) or a director. A signed copy will be retained as part of the compliance records and made available upon request by regulatory authorities.

6. Compliance Officer

6.1. Appointment of Compliance Officer

An operator shall formally appoint a senior officer at the management level as the AML/CFT Compliance Officer-Money Laundering Reporting Officer ("MLRO"). This individual must operate independently of the gaming operations and have timely access to customer identification data, transaction records, and other relevant information.

The AML/CFT Compliance Officer will have the following responsibilities:

- Designing and implementing the AML program.
- Ensuring adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing.

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

- Ensuring compliance with Targeted Financial Sanctions (TFS), including the procedure for freezing funds and other assets of designated persons or entities.
- Reviewing compliance with the casino's policies and procedures.
- Organizing training sessions for staff on compliance-related issues.
- Analyzing transactions and identifying those subject to reporting under the Ministerial Decree regarding the Indicators for Unusual Transactions.
- Reviewing all internally reported unusual transactions for completeness and accuracy.
- Maintaining records of internally and externally reported unusual transactions.
- Conducting closer investigations of unusual transactions when necessary.
- Preparing external reports of unusual transactions.
- Making necessary changes to the AML program as required.
- Remaining informed of local and international developments on money laundering and terrorist financing and making suggestions to management for improvement.
- Preparing periodic reports on the casino's efforts against money laundering, terrorism financing, and proliferation financing.

These responsibilities shall be included in the Compliance Officer's job description, and the appointed officer must formally sign and acknowledge their acceptance of these responsibilities.

The operator communicates immediately to both Curacao Gaming Control Board and FIU (MOT) the names and positions of the persons it appoints as Compliance Officer and assistants of the Compliance Officer (if applicable).

6.2. Reporting procedures

An operator must establish, record, maintain and operate reporting procedures and controls that—

- a) enable its officers, all other persons involved in its management, and all appropriate employees and workers to know to whom they should report any suspicious activity;
- b) ensure that there is a clear reporting chain to the MLRO;
- c) require an internal disclosure to be made to the MLRO if any information or other matters that come to the attention of the person handling that business are, in that person's opinion, suspicious activity;
- d) ensure that the MLRO has full access to any other information that may be of assistance and that is available to the operator;
- e) require the MLRO to consider internal disclosures in the light of all other relevant information available to the MLRO for the purpose of determining whether the activity is, in the MLRO's opinion, suspicious activity;
- f) enable the information to be provided as soon as is practicable to the Financial Intelligence Unit if the MLRO knows or suspects, or has reasonable grounds to suspect, that the activity is ML/FT; and
- g) ensure the registers as required by paragraphs 19 (registers of disclosures) and 20 (register of money laundering and financing of terrorism enquiries) are maintained and completed in accordance with those paragraphs.

6.3. Internal reporting procedures – Reporting to FIU (MOT)

1. Receiving of information from the operator's employees for knowledge or suspicion of money laundering or terrorist financing activities or relation with such activities. The information is received in a written report form ("Internal Suspicion Report");

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

2. Evaluation and examination of the information received by reference to other relevant information and discussion of the circumstances of the case with the informer and, where appropriate, with the informer's superiors. The evaluation of the information received is done on a report ("Internal Evaluation Report");
3. If following the evaluation, the Compliance Officer decides to notify FIU (MOT), they complete a written report and submit it to FIU (MOT) the soonest possible. This report is called "Compliance Officer's Report to the FIU (MOT)"
4. If following the evaluation, the Compliance Officer decides not to notify FIU (MOT), they fully explain the reasoning for their decision on the "Internal Evaluation Report".
5. Acting as the first point of contact with FIU (MOT), upon commencement and during an investigation as a result of filing a report to FIU (MOT).
6. Upon deeming a transaction or activity unusual, the Compliance Officer must ensure that the final Unusual Transaction Report (UOT) is prepared and submitted electronically to the FIU Curaçao via the goAML reporting portal within a maximum deadline of forty-eight (48) hours. This timeframe is a statutory requirement under the NORUT and must be strictly adhered to without exception.

6.4. Preparation of clients 'list

The preparation and maintenance of a list of clients categorized following a risk-based approach (Normal, High risk) which contains, among others:

- the names of clients,
- KYC documentation, and
- the date of the commencement of the business relationship.

Moreover, ensures the updating of said list with all new or existing clients, in light of additional information obtained.

6.5. Detection, recording and evaluation of risks and updating of procedures

1. Detection, recording and evaluation, at least on an annual basis, of all risks associated with existing and new clients and services, updates and amendments to the systems and procedures applied by the Firm for the effective management of the aforementioned risks;
2. Evaluation of the systems and procedures applied by a third party whom the Firm relies on for client identification and due diligence purposes;

6.6. Training

1. Acquisition of the required knowledge and skills for the improvement of the appropriate procedures for prevention and suppression of money laundering and terrorist financing;
2. Provision of advice and guidance, as well as appropriate training sessions/seminars, to the management team and employees of the Firm on matters related to the prevention and suppression of money laundering and terrorist financing.

6.7. Reporting

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

1. Money Laundering Reporting Officer is the responsible person to exercise the functions conferred by Section 7.2
2. Responding to all requests and queries from, provision of all requested information and full cooperation with FIU (MOT);
3. Maintenance of a registry which includes the following reports:
 - Internal Suspicion Report
 - Internal Evaluation Report
 - Compliance Officer's Report to the Unit for Combating Money Laundering

6.8. Prohibition of Disclosure (Tipping-Off)

In accordance with Article 11 of the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Company and all its employees, directors, and officers are strictly prohibited from making any disclosure or providing any information to the customer concerned or to any third party that an Unusual Transaction Report (UOT) or Suspicious Transaction Report (STR) has been, or may be, filed with the Financial Intelligence Unit (FIU) Curaçao.

This prohibition applies at all times. Any breach of this confidentiality obligation (tipping-off) constitutes a criminal offense under the NORUT and will result in disciplinary action up to and including immediate termination, in addition to potential civil and criminal penalties under Curaçao law.

7. Application of appropriate measures and procedures on a Risk Based Approach

7.1. Application of measures and procedures on a risk-based approach

The operator shall establish a structured Risk Matrix to classify clients into three categories: Low Risk, Medium Risk, and High Risk. The classification will be based on specific factors, including the client's geographic location, transaction behavior, and overall profile. The Risk Matrix will guide the application of appropriate controls, as follows:

- Low Risk: Simplified due diligence procedures applied, with periodic monitoring to ensure compliance.
- Medium Risk: Standard due diligence procedures implemented, including periodic reviews and ongoing assessments.
- High Risk: Enhanced due diligence measures required, including detailed verification of the source of wealth and funds, coupled with continuous transaction monitoring.

The operator applies appropriate measures and procedures, on a risk-based approach, so as to focus its effort in those areas where the risk of money laundering and terrorist financing appears to be higher.

A risk-based approach:

- I. recognizes that the money laundering or terrorist financing threat varies across clients, countries and lines of service;
- II. allows the Board of Directors to differentiate between clients of the Firm in a way that matches the risk of their particular business;
- III. allows the Board of Directors to apply its own approach in the formulation of policies, procedures and controls in response to the Firm's particular circumstances and characteristics.

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

A risk-based approach involves specific measures and procedures in assessing the most cost effective and proportionate way to manage the money laundering and terrorist financing risks faced by the Firm. Such measures and procedures are:

- I. identifying and assessing the money laundering and terrorist financing risks emanating from particular clients and geographical areas of operation of its clients;
- II. documenting in the risk management and procedures manual the policies, measures, procedures and controls to ensure their uniform application across the Firm by persons specifically appointed for that purpose by the Board of Directors;
- III. managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls.

7.2. Identification, recording and evaluation of risks

The Compliance Officer has the responsibility to identify, record and evaluate all potential risks. The successful establishment of measures and procedures on a risk-based approach requires clear communication of the measures and procedures that have been decided across the Company, along with robust mechanisms to ensure that these are implemented effectively, weaknesses are promptly identified and improvements are made wherever necessary.

A risk-based approach involves the identification, recording and evaluation of the risks that have to be managed. The Company assesses and evaluates the risk it faces, for usage of the services provided for the purpose of money laundering, terrorist financing or proliferation financing.

The Company's Business Risk Assessment (BRA) will explicitly identify, assess, and understand risks associated with, but not limited to:

- Customer Base Risk: The nature of the customer (e.g., source of wealth, geographical origin).
- Geographic Risk: Exposure to high-risk or sanctioned jurisdictions.
- Product and Services Risk: The risks inherent in the products (e.g., gambling/betting types) and services offered.
- Delivery Channel Risk: The risks associated with how products and services are accessed (e.g., online platform, payment methods, third-party agents).
- Technological Developments and New Products Risk: A mandatory assessment of ML/FT/FP risk for all new products, business practices, or technologies (including changes to payment channels or virtual assets) must be conducted and mitigated *prior to launch*.

The particular circumstances of the Company determine the suitable procedures and measures that need to be applied to counter and manage risk.

8. Design and implementation of measures and procedures to manage and mitigate the risks

When the Compliance Officer identifies the risks, it faces then they design and implement the appropriate measures and procedures for the correct management and mitigation, especially of high risk clients, which involve:

- the verification of the clients identity;
- the collection of information for the construction of their economic profile;
- monitoring of their transactions and activities;
- increased monitoring of transactions;

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

- increased levels of ongoing controls and review of relationships;
- seek additional verification information beyond the minimum requirements to substantiate client's identity;
- obtaining additional information regarding clients' source of funds and wealth;
- independently verified information;
- implementation of Board of Directors' approval of all relationships identified as high risk.
- implementation of Board of Directors' approval for exiting from an existing high-risk relationship, if risk level exceeds the entities risk tolerance;

The Compliance officer may use other reliable sources for mitigate the risk, advising Caribbean Financial Action Task Force (FATF), country assessment reports and other reports that are published by relevant international organizations.

9. Customer due diligence

9.1. *Description and Analysis*

The operator shall require government-issued identification documents for client verification, including passports, national identification cards, or driver's licenses. For clients classified as high-risk, third-party validation of these documents will be mandatory. The identification process will be reviewed and updated upon any significant changes to the client's profile or at a minimum interval of five years.

In accordance with the requirements of NORUT and the NOIS, lawyers, notaries, accountants, real estate agents, jewelers, car dealers, tax advisors and administrative offices (the new reporting entities) are required by law to identify their clients and to report any unusual transaction to the FIU (MOT) in accordance with the requirements of the NORUT and the NOIS. FIU (MOT) has issued AML/CFT directives (provisions and guidelines) for lawyers, civil law notaries, accountants, real estate agencies, tax advisors and administrative offices that allow them to implement a risk-based approach.

9.2. *Casinos*

The operator shall maintain a list of explicitly prohibited territories where online gambling is restricted, including but not limited to:

- Australia
- France
- Iran
- Iraq
- The Netherlands
- North Korea
- Singapore
- Spain
- USA and its dependencies
- Ukraine
- United Kingdom
- The Dutch Caribbean Islands: Curaçao, Aruba, Bonaire, St. Martin, St. Eustatius, and Saba

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

The operator shall ensure compliance by implementing geo-blocking of IP addresses from these territories and any other jurisdictions that do not accept the Curacao license. It is the operator's responsibility to remain informed of local laws and regulations in all jurisdictions where services are offered.

According to the NOIS, casinos are subject to customer identification requirements when they engage in financial transactions equal to or above NAf 20.000 (about USD11,173). The threshold of NAf 20.000 is too high compared to the FATF threshold of USD 3,000 for casinos. The other CDD requirements stipulated in the NOIS are also applicable to casinos. It is noted that according to the MICS casinos have the obligation to identify their customers before rendering them services for an amount higher than NAf5.000. This requirement is well under the FATF threshold of USD 3,000.

Casinos are also required to have clear customer acceptance policies which ensure that transactions will not be conducted or member accounts opened with customers who fail to provide satisfactory evidence of their identity.

9.3. DNFBPs supervised by the FIU (MOT) and GCB

While the requirements below are set out in Guidelines issued by the FIU (MOT) for DNFBPs and the GCB for casinos they are still outstanding given the OEM status of the Guidelines:

- a) The requirement in the case of legal arrangements, to take reasonable measures to understand the ownership and control structure of the customer and to identify the natural person that ultimately owns or controls the customer;
- b) The requirement to establish the purpose and intended nature of the business relationship;
- c) The requirement to conduct continuous due diligence on the business relationship and the transactions undertaken throughout the course of that relationship, to ensure that the client's records previously obtained by the service provider still reflect the client's risk profile.
- d) The requirement to ensure that documents, data or information collected under the due diligence process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of investors.
- e) The requirement to apply enhanced due diligence for higher risk clients and reduced or simplified measures for low risk customers
- f) Requirement not to apply simplified CDD measures whenever there is a suspicion of money laundering or terrorist financing
- g) The requirement for the termination of a business relationship already in existence or determining the submission of a report to the FIU (MOT) when the service provider has reasonable doubt regarding the accuracy of the data previously obtained and is unable to perform CDD measures anew.
- h) Requirement for the application of CDD measures to existing customers on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times.

10. A2F B.V. client's identification procedures

Before the provision of any services to a client, identification of a prospective client must be made from documents issued by reliable sources as prescribed in the NOIS and whenever applicable/possible the directors, representatives or Ultimate Beneficial Owners of the

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

prospective client must be interviewed personally. The operators are also required to obtain and document information on the purpose and intended nature of the business relationship with their (prospective) clients prior to offering them any services.

To prevent and combat money laundering or the financing of terrorism, the operator shall conduct standard customer due diligence which shall, at least, include the following:

- the identification of the client and the verification of the client's identity;
- the identification of the ultimate beneficiary and taking reasonable measures to verify the identity of the ultimate beneficiary in such a way that the service provider is convinced of the identity of the ultimate beneficiary;
- measures to establish the objective and the envisaged nature of the business relationship;
- conducting ongoing checks of the business relationship and the transactions carried out during this relationship, in order to ensure these, correspond to the knowledge the operator has of the client, his/her/its business and the ultimate beneficiary, as well as their risk profiles, including, if necessary, the origin of the financial resources; and, e. measures to establish whether a client is acting for him/her/itself or on behalf of a third party and taking measures to establish and verify the identity of the third party.

Furthermore, operators are encouraged to perform antecedent screening on persons subject to CDD. This could be done by e.g. searching the internationally accepted authoritative lists on the internet.

10.1. Individuals

The employees, the Agents and persons acting on behalf of the Company shall strictly comply with the CDD requirements for opening and operating of any account. No anonymous accounts or accounts in fictitious names shall be permitted, and all individuals opening an account must be over the age of 18. The Network Service Partner understands that allowing persons below the age of 18 to bet on its platform is an offense under various Relevant Laws.

The Compliance Officer shall perform CDD when:

- a) A player wagering stake, or collecting winnings (including the withdrawal of funds deposited) exceeds GBP 2,000 or more (whether the transaction is executed in a single operation or in several operations which appear to be linked); and/or
- b) A player's activity has been identified as suspicious by the Company, MLRO, the Network Service Partner or their officers and employees responsible for ensuring compliance with the AML Policy and the CDD Procedure.

If a person refuses to cooperate for a period of 28 days, even when they have been explained the reasoning behind the regulatory ask the Network Service Partner should terminate the business relationship and report the same to the MLRO or the Compliance Officer (as applicable) as withholding information is one of the "red flags" that could indicate that criminal activity has taken place and that the laundering of the proceeds of these crimes could be attempted.

Client's categories

- *High Risk clients*

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

High risk clients include:

- I. politically exposed persons;
- II. clients from countries which inadequately apply Financial Action Task Force's recommendations;
- III. correspondent banking relationships with clients from third countries;
- IV. any other client determined by the Company itself to be classified as such (please refer to appendix 1).

- *Normal risk clients*

All clients that do not fall in the low or high-risk categories are considered as normal risk clients.

Face-to-face CDD

When conducting face-to-face CDD or executing transactions for which instructions have been received on a face-to-face basis, the operator must:

1. provide a copy of the original identification document or the original transaction document with the text: "Mr. and or Mrs. appeared to me in person"; and a stamp with the prevailing date; and
2. add the signature of the client as well as the name and signature of the employee who performed the CDD or executed the transaction, to the original document.

Age Verification and Identification of (prospective) clients

The Network Service Partner does not allow customers under the age of 18 or older if local laws so stipulate as applicable to gamble and has systems and monitoring in place to ensure as far as practicable that underage customers aren't able to create accounts and gamble.

Network Service Partner shall abide by the license issuer rules and regulations pertaining to underage gambling and to any specific product rules issued by suppliers of gambling products.

If on completion of verification the customer is shown to be underage:

Their account will be frozen

The status of the account will be set to "Closed" and a note placed on the account

All wages will be treated as void and any deposits made will be refunded to the form of payment used. Where this is not possible, a parent or guardian must give details of an alternative payment method.

The verification and identification process includes:

That the customer is not able to continue with the registration until the "over 18" or "over 21" as applicable checkbox is checked.

The date of birth registration field doesn't allow for an input below the age of 18 or 21 as applicable with a pre-calculated algorithm.

Confirming the customer's identity by checking public available records where available; or

Confirming the customer's identity by having them provide a valid government-issued photo ID such as a passport or driving license when there is a suspicion that the customer is maybe underage through customer interaction and game play activity behavior, or

Warning potential customers that underage gambling is an offense

Requiring customers to affirm that they are of legal age

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

Periodically reviewing its age verification systems and implementing local industry standard improvements that may be made as technology advanced and as information improves
Ensuring that relevant staff are properly trained in the use of any age verification procedures; in particular customers services staff must be trained appropriately
Carrying out secondary age verification checks in any circumstances which give the operator reason to suspect that the person may be underage

Document verification: based on the knowledge and understanding obtained during the interactions with potential customer, the Network Service Partner shall establish the following:

B2C: In case of individuals, the Network Service Partner shall require the following:

- Full name of the customer
- Government issued identification documents containing a photograph including Passport, Social Security Card, Tax registration cards, driving license etc.
- Existing mailing and residential address along with the proof thereof.
- Contact numbers
- Nationality
- Date of Birth

B2B: For verification of the identity of the legal entity, the Network Service Partner shall require the following:

- Full business name of entity
- Business Incorporation or registration number
- Existing registered and mailing business address
- Contact details of the authorized representatives
- Date and place of incorporation and certificates evidencing the same
- Charter documents and the AML policies and procedures adopted by the company if any
- Full name, ID, Address, Date of Birth, Nationality of all Directors/Partners having executive authority of the entity.

Pursuant to article 3 of the NOIS, the identity of clients must be established through one of the following valid documents:

- a driver's license;
- an identity card issued;
- a travel document or passport;
- other document to be designated by the Minister of Finance.

Ongoing CDD

The efforts to "know your customer" must continue once the client has been identified, even after the initial identification of the client. While the on-going due diligence process must also include scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the operator's knowledge of the client, its business and risk profile, and where necessary, the source of funds. In the event that doubts relating to the identity of the client arise after the client has been accepted, the relationship with the client must be re-examined to determine

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

whether it must be terminated and whether the incident must be reported to the FIU.

The operator should apply CDD requirements to existing customers and may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction.

Examples of when it may otherwise be an appropriate time to do so is when:

- (a) appropriate scrutiny of transactions and other activities to ensure that they are consistent with the operator's knowledge of the customer, the customer's business and risk profile and source of funds for the transaction;
- (b) there is a material change in the way that the account is operated;
- (c) customer documentation standards change substantially; and
- (d) the operator becomes aware that it lacks sufficient information about an existing customer.
- (e) monitoring whether the customer or any known beneficial owner is listed on the sanctions list.
- (f) operator identifies any unusual activity, which should:
 - perform appropriate scrutiny of the activity;
 - conduct enhanced customer due diligence; and
 - consider whether to make an internal disclosure.

In the latter instances, updated copies of the identification document must be collected and retained.

Furthermore, the operator should ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of clients or business relationships.

Identification of Politically Exposed Persons

The law defines "politically exposed persons" as:

"the natural persons that have or had been entrusted with prominent public functions in the republic of Curacao or any other country, as well as their immediate family members or persons known to be close associates of such persons"

The operator has appropriate risk management in place to determine whether it's (proposed) clients are considered political exposed persons ("PEP's) and conduct enhanced due diligence for politically exposed persons (PEPs), their families and associates. The operator's decision to enter into business relationships with a PEP must be taken at its senior management level. The operator makes reasonable efforts to ascertain that the PEPs source of wealth and source of funds/ income is not from illegal activities and where appropriate, review the customer's credit and character and the type of transactions the customer would typically conduct. The operator must not accept or maintain a business relationship the institution knows or must assume that the funds are derived from corruption or misuse of public assets. Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, institutions must obtain senior management's approval to continue the business relationship. Where the operator is in a business relationship with a PEP, it must conduct enhanced ongoing monitoring on that relationship.

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

In addition, enhanced checks are applied if the country of origin of the PEP is widely known to be corrupt and where AML legislation may not be fully adhered to by the jurisdiction in question. Therefore, the operator categorizes the jurisdictions of clients and list the jurisdictions, which are considered most vulnerable to corruption e.g., those who do not apply the 40 requirements of FATF. As regards corruption, the operator uses Transparency International Corruption Perceptions index, Moneyval, IMF, FATF and World Bank as appropriate sources of information.

The meaning 'Politically Exposed Persons' includes the following natural persons who are or have been entrusted with prominent public functions' in any other foreign country:

- I. heads of State, heads of government, ministers and deputy or assistant ministers
- II. members of parliaments
- III. members of the governing bodies of political parties
- IV. members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances
- V. members of courts of auditors or of the boards of central banks
- VI. ambassadors, chargés d'affaires and high-ranking officers in the armed forces
- VII. members of the administrative, management or supervisory bodies of State-owned enterprises.
- VIII. Directors, deputy directors and members of the board or equivalent function of an international organization
- IX. Mayors

Without prejudice to the application, on a risk-sensitive basis, of enhanced Client due diligence measures, where a person has ceased to be entrusted with a prominent public function within the meaning above for a period of at least one year, the Company shall not be obliged to consider such a person as politically exposed.

None of the categories set out in above shall be understood as covering middle ranking or more junior officials. 'Immediate family members' includes the following:

- (a) the spouse or the person with which cohabit for at least one year
- (b) the children and their spouses or the persons with which cohabit for at least one year
- (c) the parents.

'Persons known to be close associates' includes the following:

- (a) any natural person who is known to have joint Beneficial Ownership of legal entities or legal arrangements, or any other close business relations, with a person referred to in above
- (b) any natural person who has sole Beneficial Ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the person referred to in above.

Without prejudice to the provisions of the Manual, the operators adopt the following additional due diligence measures when it establishes a Business Relationship or carry out an Occasional Transaction with a PEP:

- (a) the MLRO shall use a screening software to run the player's entries against sanction lists, legal regulatory directions, law enforcement lists, negative news, adverse media, local and international government records etc in respect of sanctioned persons/entities. The MLRO may use any procedures necessary to determine whether a prospective Client is a PEP. These procedures may include, depending on the degree of risk, the obtaining of information from the Client himself or from publicly available information.

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

- (b) the decision for establishing a Business Relationship or the execution of an Occasional Transaction with a PEP is taken by an Executive Director of the operator and the decision is then forwarded to the MLCO. When establishing a Business Relationship with a Client and subsequently it is ascertained that the persons involved are or have become PEPs, then an approval is given for continuing the operation of the Business Relationship by an Executive Director of the Company which is then forwarded to the MLCO
- (c) before establishing a Business Relationship or executing an Occasional Transaction with a PEP, the operator shall obtain adequate documentation to ascertain not only the identity of the said person but also to assess his business reputation (e.g. reference letters from third parties)
- (d) the operator shall create the economic profile of the Client by obtaining the information specified above. The details of the expected business and nature of activities of the Client forms the basis for the future monitoring of the account. The profile shall be regularly reviewed and updated with new data and information. The operator shall be particularly cautious and most vigilant where its Clients are involved in businesses which appear to be most vulnerable to corruption such as trading in oil, arms, cigarettes and alcoholic drinks.

The data and information that are used for the construction of the Client-legal person's economic profile shall include, inter alia, the following:

- the name of the individual
 - the country of origin
 - the permanent residential address
 - financial information – Source of Funds and Source of Wealth
 - existing banking relationships of the individual;
 - international or home country telephone directory;
 - the products that offered to the client
 - Searching the internationally accepted authoritative lists on the internet.
 - Transactional History
- (e) the account shall be subject to annual review in order to determine whether to allow its continuance of operation. A short report shall be prepared summarizing the results of the review by the person who is in charge of monitoring the account. The report shall be submitted for consideration and approval to the Board and filed in the Client's personal file.

If an individual is Suspected to be on the PEP list, we will request:

1. Player's KYC and
2. Player's ID with real time face (if needed)

Once we have the provided documents and confirm player is a PEP, we will identify the account as a PEP, ensure the account is classified as High Risk, complete the uptake of Enhanced Due Diligence (EDD) from the player and Report to MLRO if any suspicions. If not a PEP, no action is taken, but will continue to monitor.

Sanctions Policy

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

Assigned Compliance Officers will conduct screening on a weekly basis on all new players and checks through all player databases and the owners and directors of business participants. Individual's registered name, date of birth, address and locations will inspect to identify any match information from PEP & Sanction Lists.

The operator shall take reasonable measures to comply with sanctions and restrictive measures ("Sanctions") imposed on countries, territories, entities or specific persons and bodies by the United Nations, the European Union, United Kingdom as well as by the US Department of Treasury Office of Foreign Assets Control ("OFAC").

- The operator will adhere to the directives and guidance from the regulatory and other competent authorities relevant to sanctions that have a jurisdiction over operator.
- The operator will abstain from business relationships or transactions which violate or facilitate a violation of Sanctions as defined in this Sanctions Policy.
- With respect to persons and entities subject to Sanctions in general the Gaming Operator:
 - Will not establish a new business relationship
 - Will not facilitate significant transactions
 - In case of existing clients, will follow the instructions and guidelines provided by the Regulated Authority with direct jurisdiction over the operator that may require:
 - To suspend/terminate business relationship with the client;
 - To report the client/business relationship to appropriate authorities;
 - The Company could consider entering into and maintaining a business relationship with a client related to or affiliated with a sanctioned person, however such client will be subject to enhanced due diligence, frequent open source, database checks and transaction monitoring.
- The company should focus enhanced counterparty diligence and screening exercises on areas of the company's business that carry a greater likelihood of involvement with sanctions targets, or their agents, for example:
 - Where there is reasonable cause to suspect that any counterparty derives its profits from activities prohibited under international sanctions measures.

If an individual is Suspected to be on the Sanction list, we will request:

- Player's KYC and
- Player's ID with real time face (if needed)

Once the player's KYC are received, the MLRO will informed to confirm whether the player is a match with the Sanction list or not. If yes, the account will immediately be suspended, and the authorities will be informed. If not on the Sanction List, no action to be taken. The account will be monitored.

10.2. Enhanced CDD for high-risk categories of customers

Enhanced due diligence (EDD) shall be performed for all Politically Exposed Persons (PEPs), their immediate family members, and close associates. PEPs will be identified through initial onboarding and periodic screening. Relationships with PEPs must be reviewed annually, with approvals required at the senior management level. Additional documentation on source of wealth and funds must be collected and verified.

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

Enhanced due diligence would apply to the customer that is categorized as High Risk with the submission of additional information regarding their financial background and identification.

Circumstances which give rise to a client being classified as High Risk are the following:

1. When the client is a Politically Exposed Person (PEP)
2. When a client is based, operates or is in any way connected with a heightened AML risk jurisdiction
3. Clients from countries which inadequately apply FATF's recommendations
4. Where there are other reputational concerns (e.g. records or allegations of criminal activities, enforcement actions, violations or sanctions)
5. Any other case where the ultimate ownership of the client is unclear or there is suspicion of money laundering activity.
6. When a player with gross settlements/losses to bookmaker "Betfair" of a value exceeding GBP 30,000 in a rolling 365-day period;
7. A player's activity has been identified as suspicious by the Company, MLRO, the officers and employees responsible for ensuring compliance with the AML Policy and the EDD Procedure;
8. In case the company has doubts about the accuracy and completeness of any information previously obtained.

The player shall be given 28 days to provide the satisfactory documents and the account shall be frozen until satisfactory documentation is provided. Once satisfactory documentation has been received, then the member account shall be unfrozen and marked as "KYC'ed".

If a person refuses to cooperate for a period of 28 days, the business relationship will be terminated and if suspicions arise report the same to the MLRO or the Compliance Officer as withholding information is one of potential 'red flags'. That could indicate that criminal activity has taken place and that the laundering of the proceeds of crimes could be attempted.

In accordance with the latest amendments of the NORUT and the NOIS, the operator applies enhanced due diligence procedures on all high-risk clients in order to compensate the higher risk. In this respect, the employees apply one or more of the following measures:

- Ensure that the client's identity is established by additional documents, data or information
- Verify or certify the documents supplied, or requiring confirmatory certification by third party independent sources
- Take reasonable measures to establish the source of wealth and source of funds

In order to establish the source of wealth and source of funds for a high-risk client, the operator requests the following additional information:

- a. The purpose and the reason for requesting the establishment of a business relationship, and
- b. The anticipated account turnover, the nature of the transactions, the expected origin of incoming funds to be credited in the account and the expected destination of outgoing transfers/payments, and
- c. The Client's annual income (ie. wage statements, interest statements, tax returns, bank statements) the clear description of the main business/professional activities/operations, generating funds for the said person.

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

The operators are in that respect required to request their client to fill out and sign the Source of Funds Declaration Form enclosed in Appendix 3 of these AML Policy, both at the establishment of the business relationship and subsequent receipt of funds for capitalization, payments, transfers or incoming funds destined for other purposes. The Source of Funds Declaration Forms must be kept on file.

Further to the above, for high-risk clients, the operator performs the following:

- Conduct enhanced and continuous monitoring of the business relationship
- Check all High-Risk clients against equivalent online service providers and internet search engines to identify validity of passport, PEP status, involvement in any illegal activities, and inclusion in any sanctions lists.

Additional documents, data or information may be:

- **Third-party verification:** use of software or using approved third parties to conduct verification of customer documents.
- **Validation of customer documents:** Certified copies of documents to validate name, address, date of birth and source of funds of the customer/network service partners. For the purpose of validating the source of funds, the Company and/or the Network Partners (as they

case may be) shall obtain certified copies of the bank statements of the account holder of proof of business (business registration/incorporation certificate).

- **Address validation check:** Using a secure code delivered to the customer's address to validate that the customer is residing at the address stated.
- **Background and lifestyle checks:** Using open source research to obtain further information about the customer's source of wealth, occupation, property ownership status and lifestyle.
- **Source of Funds:** Confirm the immediate source from which the funds have been derived. For the purposes of confirming the immediate source of funds, certified copies of the bank statements of the customer/network partner should be obtained and reviewed.
- **Source of wealth:** Corroborate sustainable wealth that matches the customer's gambling profile. This may also overlap with responsible gambling considerations. Accurately identifying a customer's source of funds and source of wealth can be a complex process and one in which approaching an online customer directly for relevant evidence may be a last resort. Examples of sources of wealth include inheritance, investments, ownership of a business, employment etc.

For High-Risk clients the due diligence is an ongoing process, the company takes measures to ensure that the transactions of this category are consistent with the economic profile of the customer. According with the risk profile we consider that any transaction or activity is inconsistent with the economic profile of the client we report it as suspicious.

10.3. Risk-based approach

The Financial Action Task Force advises that the following range of variables will impact the level of AML/CFT risks that internet casinos face:

- Whether a casino's business model centers upon either or both of the following options:
- attracting a large number of customers who gamble relatively small amounts of money; or

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

- attracting a small number of customers who gamble relatively large amounts.
- Speed and volume of business.
- Types of financial services offered to customers.
- Types of payment and payment methods accepted from customers.
- Types of gambling offered e.g. table games, card games, and electronic games (live or automated).
- the nature of the customers - whether they are regular/frequent customers or irregular/occasional customers.
- whether the casino forms part of a bigger organization owned by the same operator, for example:
 - whether the casino operator owns and manages other land- based and/or Internet casinos;
 - whether the casino, or its operator, offers different types of gambling e.g. sports book, premium players;
 - for internet casinos, whether the operator has other web sites.
 - whether the casino is wholly based in one country, or has a presence in multiple countries, e.g. whether an Internet operator's server is in a different country from other parts of its business.
- Staffing numbers, turnover rate and experience levels.
- Type and effectiveness of existing supervision mechanisms e.g. electronic and/or physical loyalty clubs which monitor gaming activity.

10.3.1. Risk classification

The operator must develop risk profiles for all its customers to determine which categories of clients expose it to higher money laundering and terrorist financing risk. The assessment of the risk exposure and the preparation of the risk classification of a client, must take place after the CDD information

mentioned above has been obtained. The risk profile must comprise minimally the following possible categories: low, medium and high risk. The provider must apply CDD requirements to existing clients

and may determine the extent of such measures on a risk sensitive basis depending on the type of client, business relationship, or transaction.

The operator must at least consider the following risk categories while developing and updating the risk profile of a client:

- (i) customer risk,
- (ii) products/services risk,
- (iii) country or geographic risk, and
- (iv) delivery channels risk.

Customer Risk

It is important for an operator to assess the type of client and the nature and scope of the business activities of the client. The types of clients or business activities that indicate a higher risk include:

- Politically exposed persons (PEPs) and their families and associates;

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

- Transaction of significance takes place (from time to time);
- Material change takes place in the way the account is operated;
- Client documentation standards change substantially; and
- Determination of lack of or insufficient information about an existing client.

Products /Services Risk

An effective risk assessment must also include determining the potential risk presented by products and services offered by the operator. A key element is the establishment of the existence of a legitimate business, economic, tax or legal reason for the client to make use of the products/services

offered by the operator. Determining the risks of products and services must include the consideration of factors such as:

- Ability to make payments to or receive payments from unassociated or unknown third parties;
- Services where the receipt and transmission of cash proceeds are possible;
- Services to conceal beneficial ownership from competent authorities;
- Transactions or services with no apparent legitimate business, economic, tax, or legal reasons; and
- The offer by clients to pay extraordinary fees for services which would not ordinarily warrant such a premium.

Country or Geographic Risk

Country risk provides useful information as to potential money laundering and terrorist financing vulnerabilities. The following countries and territories are regarded as high-risk countries and territories:

- Countries subject to sanctions and embargoes issued by e.g. the United Nations and the European Union;
- Countries identified by FATF and FATF-style regional bodies as lacking appropriate
- AML/CFT laws, regulations and other measures; and
- Countries identified by credible sources, such as FATF, FATF-style regional bodies, IMF and the World Bank, as providing funding or support for terrorist activities that have designated terrorist organizations operating within them.

Delivery Channels Risk

Deposit and withdrawal methods are now offered from a wide variety of sources including credit/debit cards, bank transfers, wire transfers, pre-paid cards, and other methods of making deposits into and withdrawals from a customer's gaming account. These methods involve differing checks on the provenance of the funds which will have undergone due diligence to a greater or lesser degree by the payment provider. It is rare in the online gambling industry for cash deposits to be made, but, where that facility is provided, the operator must have policies and procedures in place to safeguard against the additional risk presented. The company is trying and is avoiding simply acting as banks, i.e. customers' accounts should be used to facilitate gambling, not as a substitute for conventional bank accounts.

The result of the risk assessment of a particular customer, as evidenced by the risk profile, will determine if additional information needs to be requested, if the obtained information need to be verified, and the extent to which the resulting relationship will be monitored.

11. Monitoring and improving the measures and procedures

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Clients' activities change constantly as well as the services provided. The same happens to the financial instruments and the transactions used for money laundering or terrorist financing.

The measures, procedures and controls are kept under regular review by the Compliance Officer so that risks resulting from changes in the characteristics of existing clients, new clients, services and financial instruments are managed and countered effectively.

The Compliance Officer monitors and evaluates, on an on-going basis, the effectiveness of the measures and procedures and, in general, the implementation of the risk management and procedures manual that have been introduced.

The Compliance Officer applies appropriate monitoring mechanisms which will provide them with all necessary information for assessing the level of compliance of the departments and employees of the Firm with the procedures and controls which are in force.

In the event that they identify shortcomings and/or weaknesses in the application of the required practices, measures, procedures and controls, they give appropriate guidance for corrective measures and, where deemed necessary, inform the Board of Directors.

11.1. *Effective Transaction Monitoring*

What is required is a "detailed examination of each transaction which by its nature may be considered to be particularly vulnerable to be associated with money laundering offences or terrorist financing and in particular complex or unusually large transactions and all other unusual patterns of transactions which have no apparent economic or visible lawful purpose".

In practice, where a client's instruction or transaction or behavior is not consistent with what is anticipated i.e. if it does not make sense or appears logical then an explanation must be sought by contacting the client.

If there are unexpected jurisdictions or organizations/counterparties/associates involved, again explanations should be sought.

It should be noted that failure to provide satisfactory answers or cancelling transactions when pertinent questions are asked are reasons for concern.

One main method for documenting the exercise of judgement/reasonableness during ongoing transaction monitoring is the collection of sufficient (not excessive) supporting documentation, which should be kept in the client file.

11.2. *A system of independent testing of the policies and procedures*

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

The operator maintains an adequately resourced and independent audit function to test compliance (including sample testing) with their policies, procedures and controls. The independent testing should be conducted at least annually by the internal audit department or by an outside independent party, such as the external auditor of the operator.

These tests must include amongst other:

- ✓ evaluation of the anti-money laundering and counter terrorist financing manual;
- ✓ file review of the international companies to which trust services are provided;
- ✓ interviews with employees who handle transactions and with their supervisors;

- ✓ sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- ✓ assessment of the adequacy of the record retention system.

The scope of the testing and the testing results must be documented, with any deficiencies reported to senior management and/or to the Board of Directors, and to the designated officer(s) with a request to take prompt corrective actions by a certain deadline.

12. Recognition, documentation, and reporting of unusual transactions

Gaming Operators are not only required to adhere to the stipulations of the identification regulations, but they are also required to detect and report either proposed or completed unusual transactions. Hence, it is therefore important for every operator to have adequate procedures for its personnel in place. These procedures must cover:

- a. the recognition of unusual transactions;
- b. the documentation of unusual transactions; and
- c. the reporting of unusual transactions.

12.1. Recognition of unusual transactions

An unusual transaction will often be a transaction which is inconsistent with the client's known legitimate business activities. Therefore, the first key to recognizing that a transaction or series of transactions is

unusual is to know enough about the client's or its representative's "bona fides" and potential criminal background.

Based on the NORUT legislation, objective and subjective indicators have been established by means of which operators must assess if a customer's transaction qualifies as an unusual transaction.

The operator is required to pay special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. Operators are required to examine as far as possible the background and purpose of such transactions and to set forth their findings in writing and keep these findings for at least five years

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

to assist competent authorities (e.g., supervisors, law enforcement agencies, and the FIU/MOT and auditors).

In this context, the employees of the operator that is a legal person must not only focus on the establishment of a relationship, but also on other aspects such as subsequent transactions, the frequency of the transactions, duration of existence of the client.

The operators with advanced computer information systems are encouraged to develop special programs to select objectively defined unusual transactions. Furthermore, the operator should provide its staff with specific guidance and training to recognize and document adequately the unusual transactions.

12.2. Wire transfer

Wire transfers are increasingly used for laundering funds from illegal sources. The Company must be extremely vigilant in accepting funds from its customers for transfer.

Based on FATF Special Recommendation (SR) VII26, operators must include accurate and meaningful originator information (at least the name, address and account number if existent, otherwise a unique reference number) on funds transfers on behalf of their clients within or from Curaçao and Sint Maarten

and related messages that are sent. In case the operator receives a fund transferred from a third party to the operator's client, the operator must ensure that the fund transfer information is accurate and complete. If the information seems inaccurate or incomplete, additional information must be requested prior to accepting or releasing funds²⁷. The operator must observe the latest Interpretative Note to SR VII and apply its relevant parts. The full text of the note may be consulted on FATF's website at: <http://www.fatf-gafi.org>. Also, further scrutiny is required and reporting to the FIU/MOT²⁸ must be considered.

12.2.1. The documentation of unusual transactions

To guard against money laundering and terrorist financing, it is important for the operators to provide an audit trail for suspicious/unusual funds or transactions. This must be done through documentation of all detected and reported unusual transactions.

12.2.2. Reporting of unusual transactions

The operator must have clear procedures which are communicated to their personnel for the reporting of unusual transactions.

There may be circumstances where the operator declines to establish a business relationship with a potential client or refuses to render additional services to an existing client because of serious doubts about the client's or its representative's "bona fides" and potential criminal background. While all decisions must be based on normal business criteria and the operator's internal policy to guard against money laundering and terrorist financing, it is important for the operator to provide an audit trail for suspicious activities and report all the (intended) unusual activities to the FIU/MOT without delay.

12.2.3. Internal reporting

The individual transaction or series of transactions which qualify as unusual must be reported internally without any undue delay. All transactions as mentioned in the Ministerial Decrees containing general measures regarding the Indicators for unusual transactions must be referred to the designated officers. Nevertheless, the management have been stipulate the categories of unusual transactions which must also be brought to their attention whenever available, additional documents such as copies of the identification documents, checks and account ledgers records must also be submitted as supplements. The designated officers are keeping an adequate filing system of these records.

If the compliance officer does not report internally reported transactions to the FIU/MOT, the reasons therefore must be adequately documented and signed off by this officer and/or by management.

12.2.4. External reporting

The designated officers are preparing a report of all unusual transactions for external reporting purposes. The report must be submitted to senior management for their review for compliance with existing regulations. Copies of these reports must be kept by the reporting Gaming Operator.

If an unusual transaction is not authorized by senior management to incorporate in the report to the FIU/MOT all documents relevant to the transaction including the reasons for non-authorization must be

adequately documented, signed off by the designated officer and senior management and kept by the reporting Gaming Operator.

The Company have established guidelines to the personnel to ensure that:

- the Supervisory Directors, senior management and employees do not warn customers when information about them is being reported to the FIU/MOT, or on internal inquiries being made by the institution's compliance staff on them;
- the Supervisory Directors, senior management and employees follow the instructions from the FIU/MOT to the extent that they carry out further investigation or review.

13. Record keeping

The operator ensure compliance with the record keeping requirements contained in the relevant money laundering and terrorist financing legislation. The operator should ensure that the investigating

authorities must be able to identify a satisfactory audit trail for suspected transactions related to money laundering and terrorist financing.

Where appropriate, the operators should consider retaining certain records e.g. customer identification, account files, business correspondence, and internal and external reports relative to unusual transactions of clients for periods which may exceed that required under the relevant money laundering and terrorist financing legislation, rules and regulations.

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

A document retention policy must include the following:

- All necessary records on transactions carried out in the course of gambling business must be maintained for at least five years after the transaction takes place. Such records must be sufficient to permit reconstruction of individual transactions (including the including identification information, account files, business correspondence records and the result of any analysis undertaken) so as to provide, if necessary, evidence for prosecution of criminal behavior.
- Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence must be kept for at least five years after the business relationship has been discontinued.
- The operator should ensure that all customer and transaction records and information are available on a timely basis to the domestic competent authorities.

In situations where the records relate to on-going investigations or transactions which have been the subject of disclosure to the FIU/MOT, investigating or law enforcement authority, they must be retained until it is confirmed by these parties that the case has been closed.

13.1. Time period of keeping documents / data

The above documentation /data is kept throughout the period that the Firm maintains a business relationship with the client and for a period of at least five (5) years from the date on which the relevant business or activities taking place in the course of which transactions were completed.

In the case that one of the Firm's clients is under investigation by FIU (MOT), all relevant documentation /data is kept until FIU (MOT) confirms that the investigation has been completed and the case has been closed.

13.2. Format of records

The retention of documentation /data, other than original documents or certified true copies that are kept in a hard copy form, may be in other forms, such as electronic form. However, if requested, records concerning client identification and details of transactions should be made available for use as evidence in any possible investigation into money laundering and terrorist financing in a visible and legible form.

13.3. Certification and language of documents

The documentation /data obtained should be in their original form or in a certified true copy form. In the case that the documentation /data is certified as true copy by a different party than the Firm itself or by the third party the documentation /data must be apostilled or notarized. Name and signature of person certifying documentation / data, as well as date of certification must be included.

A true translation must be attached in the case that the above documentation /data is in a language other than English.

13.4. Description and analysis

The intentional violation of record-keeping requirements is punishable with either, a fine of up to NAf. 500,000 (US\$ 280,000), or imprisonment of up to four (4) years, or both (Article 10 paragraph 1 of the NOIS). The unintentional violation of record-keeping requirements is punishable with either, a fine of up to NAf. 250, 000 (US\$ 140,000), or imprisonment of up to one (1) year, or both (Article 10 paragraph 2 of the NOIS). Punishment is pronounced either against the legal entity, or against those who ordered the act to be committed, or against both (Article 53 of the Penal Code (Article 53 and 96 of the Penal Code together with Article 10 of the NOIS)).

Financial institutions are required to comply with instructions from their supervisory authorities (Article 22h, paragraph 3 of NORUT; Article 22 of NOSBCI; Article 11, paragraph 3 of the NOIS).

14. Employees' obligations, education and training

The Gaming operator should develop training programs and provide (ongoing) training to all personnel who handle transactions that may be qualified as unusual or suspicious based on the indicators outlined in the Ministerial Decree regarding the Indicators for Unusual Transactions (N.G. 2010, no. 27).

Training must at least address the following:

- creating awareness by the employee of the money laundering and terrorist financing issue, the need to detect and deter money laundering and terrorist financing, the laws and regulations in this respect and the reporting requirements;
- the detection of unusual transactions or proposals, and the procedures to follow after identifying these;
- making sure that the need to verify the identity of the client is understood; and
- the developments in the area of money laundering and terrorist financing.

As far as new employees are concerned, training must be provided to all new employees dealing with clients, irrespective of their level of seniority. Similarly, training must also be provided to existing members of the staff (such as account and assistant account managers) who are dealing directly with clients. These persons are the first point of contact with potential money launderers and terrorists and their efforts are therefore vital to the organization's strategy in curtailing money laundering and terrorist financing.

A higher level of instruction covering all aspects of money laundering and terrorist financing policies, procedures and regulations must be provided to those with the responsibility to supervise or manage the staff.

In addition the operator should make arrangements for refreshment training at regular intervals to ensure that the staff members do not forget their responsibilities and that they are updated on current and new developments in the area of money laundering and terrorist financing techniques, methods and trends. The training must include a clear explanation of all aspects of the laws or executive decrees relating to money laundering and terrorist financing and requirements concerning customer identification and due diligence. This might be best achieved by an annual review of the instructions for recognizing and reporting of unusual transactions.

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

In order for the operator to be able to demonstrate that it has complied with the aforementioned guidelines with respect to training, it must at all times maintain records which include:

- details of the content of the training programs provided or training programs followed
- the names of the person(s) who have received the training;
- the date on which the training was provided;
- the results of any testing carried out to measure the participants' understanding of the money laundering and terrorist financing requirements; and
- an on-going training plan.

The Compliance Officer ensures, by introducing a complete employee's education and training program, that all employees are fully aware of their legal obligations according to:

- The systems and procedures described in the present manual;
- The NORUT, article 22h, paragraph 3;
- The NOIS, article 2, paragraph 5, and article 11, paragraph 3; and
- Regulations for Foreign Exchange Transactions Curaçao and Sint Maarten (N.G. 2010, no.112), article 21, paragraph 1. System for the purpose of money laundering and terrorist financing.

15. Offences and Sanctions in the NORUT and the NOIS

An operator that does not comply with the compulsory AML/CFT requirements is committing an offence, which is an unlawful and punishable act. The way in which an offence is punished

depends on the severity of the offence committed. Offences are subdivided in: misdemeanors and felonies.

In accordance with article 22a, paragraph 1 and article 22b paragraph 1 of the NORUT, the Supervisory Authority has the authority to impose a penalty or an administrative fine on the Operator that does not or does not timely comply with the obligations imposed by or pursuant to article 11, article 12 paragraph 2, article 13, and article 22h, paragraph 3.

Pursuant to article 9, paragraph 1 and article 9a paragraph 1, of the NOIS the Supervisory Authority has the authority to impose a penalty or an administrative fine on the Operator that does not or does not timely comply with the obligations imposed by or pursuant to article 2, paragraphs 1, 2, 5, article 3, paragraphs 1 through 6, article 5 paragraph 1 through 4, articles 6, 7, 8 and article 11, paragraph 3.

The amount of a penalty or fine for the various offences is specified in the National Decree on the non-compliance penalties and administrative penalties for reporters of unusual transactions (ND PFRUT) (NG 2010, no. 71) and the National Decree Penalties and Fines Service Providers (ND PFSP) (NG 2010, no. 70).

The Supervisory Authority will report an offence to be criminally investigated or prosecuted by the law enforcement in circumstances where the offender emphatically refuses to comply with the NORUT and/or NOIS.

15.1. Penalties related to the NORUT and the NOIS

The violation of the obligations imposed by or pursuant to the following articles is subject to a maximum penalty of NAf. 500,000.

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

Based on abovementioned article 22h, paragraph 3, NORUT and article 11, paragraph 3, NOIS the compulsory requirements in the Provisions and Guidelines are also subject to a maximum penalty of NAf. 500,000. A list of these requirements is included in Appendix I to the Policy Rule on the violation of the NORUT and NOIS legislations and the AML/CFT provisions and guidelines of the Supervisory Authority. It concerns all the provisions that the regulated entity “must” comply with.

The Supervisory Authority will indicate in the Decree to impose a penalty the term in which the violator can execute a mandate without a penalty being forfeited.

The amount due can be collected by way of a writ of execution, increased by the costs falling on the collection. The writ of execution shall be served on the violator by means of a bailiff's notification and will produce an entitlement to enforcement.

15.2. *Administrative fines related to the NORUT and the NOIS*

The violation of the obligations imposed by or pursuant to the following articles is subject to a maximum administrative fine of NAf. 1000.

Based on the abovementioned article 22h, paragraph 3, NORUT and article 11, paragraph 3, NOIS the compulsory requirements in the Provisions and Guidelines are also subject to a

maximum administrative fine of NAf. 1,000. A list of these requirements is included in Appendix I to this Policy Rule. It concerns all the provisions that the regulated entity “must” comply with. Before proceeding to imposing a penalty, the Supervisory Authority shall inform the regulated entity “in writing of the intention to impose a penalty, stating the grounds on which the intention is based, and shall offer him the opportunity to redress the omission within a reasonable term.

15.3. *Referral for criminal investigation in accordance with the NORUT/NOIS*

The Supervisory Authority will refer an offence for criminal investigation or prosecution to the law enforcement in circumstances where the offender emphatically refuses to comply with the compulsory requirements set out in the NORUT and/or NOIS.

In case of violation of or acting contrary to the provisions in the relevant articles mentioned in article 23 NORUT, or violation of regulations set by or pursuant to the relevant articles mentioned in article 10 NOIS, and the compulsory requirements in the Provisions and Guidelines the Central Bank may immediately refer the violation to the Public Prosecutor for further (criminal) investigation and prosecution. An example of a case where the Central Bank may immediately refer the violation to the Public Prosecutor for further (criminal) investigation and prosecution is that the Central Bank, during an onsite examination, takes notice of serious or grave violation of the NORUT, NOIS or the Provisions and

Guidelines. Furthermore, if the supervised regulated entity “does not comply with its obligations, even after an increased penalty or administrative fine, the Central Bank can refer the violation for further investigation to the Public Prosecutor, by providing them with the relative documents.

Appendix 1: Glossary/Definitions

Board of Supervisory Directors

The governing body of a Gaming Operator, elected by the shareholders, to oversee and supervise the management of the institution's resources and activities. They are ultimately responsible for the conduct of the institution's affairs, and control its direction and, hence its overall policy.

Caribbean Financial Action Task Force (CFATF)

The CFATF is an organization of twenty-six states of the Caribbean basin, which have agreed to implement common countermeasures to address the problem of criminal money laundering. CFATF was established as a result of meetings convened in Aruba in May 1990 and in Jamaica in November 1992. The CFATF maintains a website at: <http://www.cfatf.org/>

Certify means to declare formally that a certain stated fact is true.

Client or customer

Pursuant to article 1, sub c of the NOIS, a client/customer is anyone to whom a financial service, as defined in article 1 sub b of the NOIS, is rendered.

Financial Action Task Force on Money Laundering (FATF)

The FATF is an inter-governmental body established in 1989, and whose purpose is to develop and promote policies to combat money laundering and terrorist financing. It has 29 member countries and two regional organizations. It works in close cooperation with other international bodies involved in this area such as the United Nations Office for Drugs Control and Crime Prevention and the CFATF. The FATF maintains a website at: <http://www.fatf-gafi.org/>

High-risk and non-cooperative jurisdictions are jurisdictions that have detrimental rules and practices in place which constitute weaknesses and impede international co-operation in the fight against money laundering and terrorism financing.

Identify means to establish the identity of someone.

Know Your Customer (KYC)

The objective of KYC policies and procedures of a Gaming Operator is for them to know the customer with whom they are dealing, especially their regular customers. Sound KYC policies and procedures are critical in protecting the safety and soundness of the Company and the financial system.

NOIS

The National Ordinance on the Identification when Rendering Financial Services includes provisions on the identification of clients when rendering financial services.

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

Misdemeanor is a minor crime which is punishable.

Politically exposed persons (PEPs)

As defined in Customer due diligence for banks (Basel publication 85- October 2001), politically exposed persons (PEPs) are individuals who are or have been entrusted with promoting public functions, including heads of state or of governments, senior politicians, senior government, judicial or military officials, senior executives or publicly owned corporations and important political party officials.

Office of Foreign Assets Control (OFAC)

Office of Foreign Assets Control of the U.S. Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction.

The Unusual Transaction Reporting Center (FIU/MOT)

Pursuant to article 11 of the National Ordinance on the reporting of Unusual Transactions (N.G. 1996, no. 21), any (legal) person who provides a financial service is obliged to inform the “Meldpunt Ongebruikelijke Transacties” FIU/MOT of an unusual transaction which is contemplated or has taken place.

Source of funds refers to the activity that generated the funds for a client to be deposited into an account. This may include e.g. salary bonuses, earned income, interest and dividend payment.

Source of wealth refers to the activity that generates or which have generated an individual's net financial position.

Verify means to confirm; to establish the truth, accuracy or reality of something.

(Ultimate) beneficial ownership

Refers to the natural person(s) who ultimately own(s) or control(s) a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person.

Appendix 2: Internal Reports for Money Laundering

INTERNAL SUSPICIOUS REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

REPORTER'S DETAILS

Name: _____ Tel: _____
Department: _____ Fax: _____
Position: _____

CLIENT'S DETAILS

Name: _____
Address: _____
Tel: _____ Date of Birth: _____
Fax: _____ Occupation: _____
Details of Employer: _____
Passport No.: _____ Nationality: _____
ID Card No.: _____ Other ID Details: _____

INFORMATION / SUSPICION

Brief description of activities/transaction: _____

Reason(s) for suspicion: _____

Reporter's Signature

Date

FOR COMPLIANCE OFFICER' USE

Date Received: _____ Time Received: _____ Ref: _____
Reported to FIU: Yes/No _____ Date Reported: _____ Ref: _____

INTERNAL EVALUATION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

Reference: _____	Clients Name: _____
Reporter: _____	Department: _____
<u>Enquiries Undertaken (Brief Description)</u>	

<u>Documents attached</u>	

<u>Compliance Officer's Decision</u>	

_____	_____
Compliance Officer's Signature	Date

Compliance Officer's report to the FIU (MOT)

I. GENERAL INFORMATION

Name of reporting firm:

Address, telephone and fax
numbers:

Date when business relationship started or one-
off transaction was carried out:

Type of services offered to client:

II. DETAILS OF NATURAL PERSON(S) INVOLVED IN THE SUSPICIOUS TRANSACTION(S) / ACTIVITY(IES)

NATURAL PERSONS

Name:

Residential address:

Business address:

Occupation:

Date and place of birth:

Nationality and passport number:

III. FULL DESCRIPTION AND DETAILS OF TRANSACTIONS / ACTIVITY AROUSING SUSPICION

IV. REASONS FOR SUSPICION

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING: GUIDELINES

V. OTHER INFORMATION

Client's accounts with domestic, international or foreign banks (if known)

Other information the firm wishes to bring to the attention of FIU(MOT) (if any)

COMPLIANCE OFFICER'S signature:

Date:

NB: The above report should be accompanied by photocopies of the following:

1. For natural persons, the relevant pages of clients' passports evidencing identity.
2. All documents relating to the suspicious transaction(s)/activity(ies)

Appendix 3: Source of Funds Declaration Form

To: (name of ultimate beneficial owner of the international company)

Time:

Date:

1) I, _____ understand that I am making this declaration for my own protection as well as for the protection of the company (trust) service provider that provides trust services to the international company I (co-)own.

2) I declare that the funds totaling _____, which have been used to purchase interest in _____ (name of international company) represent funds obtained by the undersigned from the following source(s):

3) The undersigned is aware that the information contained in this Source of Funds Declaration Form may be disclosed to those institutions which are legally entitled to the information contained here.

Ultimate Beneficial Owner's name

Ultimate Beneficial Owner's address

Ultimate Beneficial Owner's Signature


.....

Marcin Juliusz Wasik
Director