

MTech Ventures B.V.

POLICY

on Prevention of Money Laundering, Terrorist Financing and Proliferation Financing

Document Information:

Approval	Managing Director
Responsible Office	Compliance Officer
Review	Annually
Audience	All Employees, Contractors, and Third Parties
Effective Date	April 10, 2025
Next Review Date	May 30, 2026

Version Control:

Date	Version	Summary Changes	Approved by Management
March 28, 2024	1.0	Policy implementation	
April 10, 2025	2.0	Policy update in line with CGA AML Regulations	Guardian Corporation Curacao B.V. obo MTech Ventures B.V. 29 May 2025 

For questions regarding this Policy please contact:

Compliance Officer: Georgios Papastylanou

Table of Contents

1.	POLICY STATEMENT	3
2.	PURPOSE OF THE POLICY.....	3
3.	MONEY LAUNDERING AND TERRORIST FINANCING RISKS	4
4.	DEFINITIONS	5
5.	POLICY IMPLEMENTATION.....	7
A.	RESPONSIBILITY OF THE SENIOR MANAGEMENT	7
B.	AML & TF COMPLIANCE OFFICER	7
C.	EMPLOYEES	8
I.	STAFF RELIABILITY AND PROBITY	8
II.	PROFESSIONAL SUPPORT AND TRAINING	8
6.	CONTROL ENVIRONMENT	9
A.	BUSINESS RISK ASSESSMENT.....	9
B.	CUSTOMER RISK ASSESSMENT	9
C.	CUSTOMER ACCEPTANCE POLICY	10
I.	PROHIBITED CATEGORIES OF CUSTOMERS	10
II.	RISK INDICATORS	10
III.	CUSTOMER DUE DILIGENCE (CDD) MEASURES.....	11
IV.	POLITICALLY EXPOSED PERSONS (PEPS)	11
V.	SANCTIONS SCREENING	11
7.	CUSTOMER DUE DILIGENCE (CDD)	12
A.	IDENTIFICATION AND VERIFICATION OF THE PLAYER	12
B.	IDENTIFICATION AND VERIFICATION OF THE BENEFICIAL OWNER	13
A.	TIMELINE FOR COMPLIANCE AND NON-COMPLIANT DOCUMENTS	13
B.	ENHANCED DUE DILIGENCE (EDD)	14
C.	TARGETED FINANCIAL SANCTIONS	14
9.	MONITORING.....	16
A.	MONITORING OF THE ACCOUNT ACTIVITIES.....	16
B.	TRANSACTIONS MONITORING.....	16
10.	REPORTING UNUSUAL ACTIVITIES AND TRANSACTIONS	19
A.	INDICATORS OF UNUSUAL TRANSACTIONS	19
B.	PROHIBITION OF DISCLOSURE.....	19
C.	PROTECTION FOR REPORTING EMPLOYEES.....	19
11.	RECORD-KEEPING.....	20
	COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE	21
12.		21

1. POLICY STATEMENT

The Policy on Prevention of Money Laundering, Terrorist Financing and Proliferation Financing (hereinafter — the Policy) outlines the general unified standards and procedures of anti-money laundering and combating terrorism financing which must be adhered by MTech Ventures B.V. , a Curacao-based operator of offshore games of chance (hereinafter — the Company).

It shall be the responsibility of the Company to inform expected standards of Anti-Money Laundering requirements to its authorized operators and provide the copy of this Policy for implementation. It may obtain certification from its Authorized Operators on a quarterly basis confirming compliance to this Policy and applicable AML requirements.

This Policy provides generic guidance on Anti-Money Laundering requirements broadly in line with industry norms and requirements applicable to gaming industry. However, every entity named above and to which this Policy applies must note applicable local AML regulations from time to time and adhere to it.

In any country or jurisdiction where the applicable anti-money laundering and terrorist financing laws and regulations require the Company's companies to establish higher standards, such country standards must be adhered to.

Compliance with this Policy is mandatory and essential for ensuring that Company Companies fully comply with applicable anti-money laundering and terrorism financing laws and regulations of respective countries and jurisdictions.

The Company is committed to annual review and critical reassessment of this Policy in light of its business strategies, goals and objectives on an ongoing basis.

2. PURPOSE OF THE POLICY

The purpose of this Policy is to establish a clear and structured framework that enables the Company to detect, prevent, and report any activities relating to money laundering, terrorist financing, and proliferation financing. This Policy articulates the minimum standards, roles, and responsibilities required to ensure compliance with all relevant legal and regulatory obligations under the jurisdiction of Curaçao.

The following laws and regulations, as well as any additional regulations issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law, are applicable to the Company:

- National Ordinance of the 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157);
- Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- National Decree for general measures, of the 10 July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10 July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094

(2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30);

- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- Curaçao Gaming Control Board Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025.

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

These laws and standards oblige the Company to adopt risk-based procedures for customer due diligence, monitoring of transactions, and reporting of unusual activities.

By implementing this Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy, the Company aims to ensure that all employees understand and fulfill their legal and regulatory obligations. The Company will apply a risk-based approach to customer due diligence, transaction monitoring, and the reporting of unusual activity. Additionally, this Policy seeks to foster a culture of compliance, transparency, and accountability across all levels of the organization.

From a business perspective, this Policy aims to protect the integrity of the Company's operations by preventing the platform from being exploited by criminal actors. It also seeks to safeguard the Company's reputation with customers, financial institutions, and regulatory authorities. Furthermore, maintaining eligibility for operating licenses and business partnerships is a key objective, as the Company demonstrates compliance with relevant regulations. Finally, this Policy is designed to ensure business continuity by mitigating the legal, financial, and operational risks associated with AML/CTF breaches.

3. MONEY LAUNDERING AND TERRORIST FINANCING RISKS

As any other online funds recipient and processing business, the Company is exposed to a variety of risks related to a potentially improper use of the its business facilities in the interests of those involved in money laundering and terrorist financing. While these risks are inherent and cannot be entirely avoided, the Company believes that the risks could be identified and contained via effective use of the AML&TF procedures, systems and personnel.

The key ML & TF risks.

1. The risk of accepting the customers whose identities and/or addresses are hidden to conceal the direct relation to ML&TF activities (for example, use of multiple passports to conceal the true identity or residential address.)
2. The risk of taking, as a deposit for online gaming via the Company's website, the funds that have, unbeknownst to the Company, been originated from illegal and/or terrorist-supporting sources (for example, transfer of gambling funds directly or indirectly from FATF-censured jurisdictions.)
3. The risk of providing an unintended financial conduit or repository for the funds originated in the course of illegal and /or terrorist-supporting activities (for example, temporary "parking" of funds without the direct use in e-gambling activities.)
4. The risk of the illegal funds transfers (withdrawal) by the customers via the Company's website facilities (for example, placing the funds without intention of using them in betting activities).

5. The risk of unknowing conduct, by the Company, of certain functions of a financial institution for any of the customers beyond the usual business remit (for example, by saving, exchanging or transferring the customer funds at the customer requests).

The Company recognizes that in addition to the aforementioned risks there may exist various other unknown sources of ML&TF threats to the business. While identification and prevention of such threats is beyond the Company's normal business capacity, the management believe that fostering the general alertness, risk awareness and the spirit of constructive scepticism among employees is the best general preventive measure that could prevent ML&TF risks from materializing.

In view of the management, ML&TF risks and business risks are intertwined inextricably hence assessment of ML&TF risks is a part of the systematic risk assessment regularly conducted by the Company's management.

4. DEFINITIONS

CFATF means The Caribbean Financial Action Taskforce, an organization of twenty-four (24) states of the Caribbean Basin, Central and South America, which have agreed to implement common countermeasures to address money laundering.

Compliance Officer means A senior officer at management level and independent from the games' operations, responsible for the detection and deterrence of money laundering and terrorist financing.

FATF means The Financial Action Task Force. An independent intergovernmental body, established in 1989 and mandated by its Member Jurisdictions to develop and promote policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

FATF Recommendations means A framework of recommendations on policies and measures, issued by the FATF, to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction;

Financial Transactions include the purchase or cashing in of casino chips or tokens, the opening of an account, wire transfers and currency exchanges. Financial transactions do not refer to gambling transactions that include only casino chips or tokens. Amounts wagered and winnings are considered as gambling transactions. Gambling transactions are not considered as financial transactions.

Financing of proliferation (PF) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

FIU means The Financial Intelligence Unit Curaçao, referred to in art. 2 of the NORUT.

Kingdom Sanctions Act means The National Ordinance also known as the "Rijkssanctiewet", published under N.G. 2016 no. 54.

Money laundering (ML) is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Money laundering may generally occur in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from illegal or criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

NOIS means National Ordinance on Identification of Clients when rendering Services (Landsverordening identificatie bij dienstverlening, N.G. 2017, no. 92).

NORUT means National Ordinance on the Reporting of Unusual Transactions (Landsverordening Melding Ongebruikelijke Transacties, N.G. 2017, no. 99).

Politically Exposed Persons (PEPs) means Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country and the direct family members or close associates of such persons. Examples are: Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

Sanctions National Ordinance means The National Ordinance also known as the "Sanctielandsverordening", published under N.G. 2014 no. 55.

Source of Funds Refers to how the funds for a particular transaction were obtained by the player, like personal savings, pension release, property sales, share sales and dividends, gambling winnings, gifts, compensation from legal rulings.

Source of Wealth is the origin of all the money a person has accumulated over their lifetime, like employment income, inheritances, investments, business ownership interests.

Targeted financial sanctions are measures imposed by governments or international bodies to restrict the financial activities of specific individuals or entities linked to unlawful activities, such as terrorism or money laundering. These sanctions aim to prevent these parties from accessing the financial system. Unlike general sanctions that apply broadly to entire countries, targeted sanctions focus on specific individuals or entities. This approach minimizes the impact on the wider population while addressing particular risks. Targeted financial sanctions apply to individuals or entities listed on sanctions lists maintained by organizations like the United Nations or the European Union.

Terrorism Financing (TF) refers to the provision of funds or financial support for terrorist acts, individuals, or organizations, and is characterized by the intent to intimidate populations or compel governments and international bodies to act or refrain from acting. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, possibly for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money, such funding could be of cumulative nature over extended periods, and the associated transactions may not be complex.

Unusual transaction A transaction that is considered as such on the basis of certain indicators, pursuant to Article 10 of the NORUT.

(Ultimate) beneficial ownership (UBO) 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.

5. POLICY IMPLEMENTATION

The Company internal controls are a set of policies and procedures aimed at securing the efficient and compliant business within the Company and provision of the safe and fair gambling environment for the customers.

Overall logic of the internal controls at the Company is described in the Business Risk Assessment, hereafter referred to as Operating Control Matrix (presented in Appendix A). The Matrix is a practical guidance on various controls mandatory for execution in the course of the daily business of the Company. Periodically, the matrix is updated on an annual basis to reflect the changing business requirements and regulatory changes in the markets in which the Company operates.

Internal controls in relation to ML&TF risks consist primarily of systematic application of the rules and procedures laid out in the corresponding sections of this Policy and the Regulations.

a. RESPONSIBILITY OF THE SENIOR MANAGEMENT

The Senior Management is responsible for:

- setting and approving the general principles underlying the Policy for Prevention and Combatting of Money Laundering and Terrorist Financing
- appointing Compliance Officer and Deputy Compliance Officer and communicating to them the internal policies
- defining the duties and responsibilities of the Compliance Officer and Deputy Compliance Officer
- ensuring that effective and sufficient systems and controls are in place to enable compliance with all rules and regulations
- ensuring that the Compliance Officer and Deputy Compliance Officer have completed and timely access to all data required to effectively undertake their duties including, but not restricted to, data concerning customer identity, transaction documentation and other relevant information maintained
- ensuring that all employees are aware to whom they have to report any information concerning unusual transactions
- ensuring that the Compliance Officer and Deputy Compliance Officer have sufficient resources including competent staff and technological equipment
- assessing and approving the annual report and taking appropriate actions to remedy any weaknesses and/or deficiencies identified in the annual report.

b. AML &TF COMPLIANCE OFFICER

TIYE-TAMUNONAKIKA MICHELLE MCBAWO-BRIGGS, is appointed as Compliance Officer with effect the 25.03.2024

The Compliance Officer has working knowledge of the Company's business environment, risks inherent to the Company's business model and AML&TF provisions as stipulated in the Regulations as amended. AML&TF Compliance Officer also performs the duties of Money Laundering Reporting Officer and is responsible for reporting transactions unusual from AML&TF standpoint to Senior management in accordance with Section RESPONSIBILITY OF THE Senior Management hereof.

General duties of the AML&TF Compliance Officer include monitoring of the Company's compliance with the AML&TF obligations, assessment of the business risks both internal and external, oversight of the AML&TF related communication and training for employees and reporting of the findings and critical issues of the AML&TF systems and procedures to the managers and executives of the Company.

The AML&TF Compliance Officer is vested with full responsibility and authority to enforce the AML&TF Policy and working procedures. Responsibilities of AML&TF Compliance Officer

- Spearheads the global AML&TF and is responsible for the Company's overall AML&TF strategy and policies.
- Conducts escalation and sanctioning in cases of internal non-compliance or lack of quality with AML&TF strategy and policies.
- Represents AML&TF activities at the Company's Senior Management level.
- Manages central AML&TF function of the Company and controls adequacy of policies, organizational structure and resources devoted to AML&TF compliance.

- Drives communication to the Board and other stakeholders with respect to issues concerning AML&TF compliance.
- Maintains relationships between AML&TF function and the Company's external auditors, regulators and other compliance authorities.
- Oversees and presents to the Board overview and budget of the AML&TF activities on a yearly basis.
- Contributes to the elements of the IT-systems related to AML&TF compliance.
- Presents to Senior Management the yearly AML&TF Compliance Report.
- Reports to Senior Management all cases of non-compliance or inadequate compliance with AML&TF policies and procedures on ongoing basis, together with recommendations for improvement.

c. EMPLOYEES

i. STAFF RELIABILITY AND PROBITY

The Company has established HR policies and procedures for effective initial candidate screening and ongoing employee management. All personnel undergo a personal identification process, and candidates must complete an ID profile that includes psychological tests during their first interview to assess potential risks. After the initial interview, successful candidates participate in a second interview with the HR Director, followed by discussions with the subject area manager and a member of the internal security department. A thorough background check is conducted, which includes contacting previous supervisors, verifying criminal records, and reviewing job references.

Once candidates successfully complete the screening process, they are required to undergo a mandatory three-week introductory training course divided into five stages, covering bookmaking basics, payment systems, software usage, customer complaint handling, and workplace training. After passing all exams, new employees begin their roles under close supervision. For executive positions, candidates must have a personal interview with the CEO or owner before a hiring decision is made.

ii. PROFESSIONAL SUPPORT AND TRAINING

The Company is committed to supporting employees' professional development through various training opportunities, including on-site and remote training, technical seminars, and workshops. Employees receive training in relevant business areas, with management training focusing on effective management practices and business English courses available for all staff. Specialized professional upgrade courses are conducted internally for Trading and Operational Department staff, while the Marketing and Finance Departments participate in targeted training sessions relevant to their fields.

In addition, refresh training sessions are conducted periodically, at least annually, to ensure employees remain up-to-date with current practices. Specific events, such as the introduction of new systems or technologies—especially those that have a higher potential for misuse in money laundering—will trigger additional training sessions. Significant violations of this policy will also prompt targeted training to reinforce compliance expectations.

Additionally, the Compliance Officer conducts mandatory introductory Anti-Money Laundering and Terrorism Financing (AML&TF) training for all new employees, which covers their roles in compliance, identifying red flags for money laundering, and the procedures for reporting suspicious activities. This training is supplemented with updates on the latest tools and practices in AML&TF investigations. The Compliance Officer maintains a register of all trained employees involved in monitoring transactions and compliance management.

-

6. CONTROL ENVIRONMENT

a. BUSINESS RISK ASSESSMENT

The Company recognizes the requirement for all casinos to conduct a comprehensive Business Risk Assessment (BRA) to identify the money laundering (ML) and terrorist financing (TF) risks they may be exposed to. This assessment ensures that the policies, controls, and procedures in place are adequate to prevent and mitigate these risks. It specifically addresses how the Company's products and services could be misused for money laundering, financing terrorism, and financing proliferation, as well as the extent of those risks.

In conducting the BRA, the Company takes into account all relevant factors that may impact the risks of money laundering, financing of terrorism, and financing of proliferation. Special consideration is given to the types of customers, the products and services offered, the delivery channels, and geographical risk factors. The effectiveness of these measures is continuously monitored, and improvements are made as necessary.

The Company revises its business risk assessment whenever there are changes in the operational environment or business activities, such as the introduction of new payment methods, entry into new markets, the launch of new games, or changes in regulations. In the absence of significant changes, the business risk assessment is reviewed at least annually to evaluate whether updates are necessary.

This risk assessment is documented and must be approved by the Board of Directors. It should also be made available to the Gaming Control Board (GCB) upon request. The documentation includes the following aspects:

- The methodology adopted for the assessment
- The rationale for categorizing risk factors as low, medium, or high
- The outcomes of the BRA
- Any information sources utilized in the assessment

To operate on a risk-based approach, the Company commits to staying informed about the latest developments regarding money laundering and terrorist financing, ensuring that its policies and procedures remain effective and aligned with regulatory expectations.

b. CUSTOMER RISK ASSESSMENT

The Customer Risk Assessment procedure is a crucial component of the internal Anti-Money Laundering (AML) program at the casino, designed to evaluate the specific risks associated with providing services or products to customers. The assessment begins when a new customer applies for an account, at which point their risk profile is formulated based on the information collected. The initial Customer Risk Rating assigned helps determine the frequency and intensity of ongoing reviews; higher-risk customers will be subject to more frequent and rigorous monitoring.

The assessment process considers several key factors:

- o **Customer Risk:** This involves evaluating the customer's background, occupation, and transaction patterns. Higher-risk categories include customers with multiple or irregular income sources, politically exposed persons (PEPs), high spenders, disproportionate spenders (whose spending habits do not align with their known income), and those using third parties to gamble in ways that may circumvent customer due diligence measures.
- o **Product/Service Risk:** This factor assesses the risks associated with the casino's offerings. Certain gaming products or services, especially those allowing customers to influence outcomes, pose higher risks. Payment methods are also evaluated, with specific high-risk factors including anonymous payment options (like pre-paid cards and virtual assets), unusual account usage, peer-to-peer gaming, and multiple accounts or wallets. Additionally, identity fraud and the use of unlicensed electronic wallets are considered significant risks.
- o **Geographic Risk:** The geographic location of the customer and the transaction is assessed, with higher risk assigned to customers from countries with weak AML regulations or high corruption levels. Relevant sources of information include the FATF lists of high-risk jurisdictions, the U.S. Department of State's International Narcotics

Control Strategy Report, and other credible indices. The nationality, residence, and place of birth of the player are also taken into account.

- o **Delivery Channel Risk:** This involves evaluating the methods used to establish a business relationship or conduct transactions. Channels that favor anonymity and non-face-to-face interactions are considered higher risk, prompting the Company to implement reasonable measures to mitigate these risks.

After the assessment, customers are categorized as low, medium, or high risk. The level of due diligence and ongoing monitoring applied corresponds to their risk classification:

- For customers assessed as low risk, a Simplified Due Diligence process will be applied, provided they do not exhibit any risk-enhancing characteristics and their transactions remain below the threshold of Cg. 4,000.
- Medium and high-risk customers will require additional information and documentation in accordance with the Company's policies.
- Accounts classified as high risk or displaying potentially suspicious behavior will be reviewed by compliance personnel and reported to the Compliance Officer (CO) for further investigation.

This structured approach ensures that the casino effectively identifies and mitigates the risks associated with its customers, aligning with regulatory expectations and promoting a robust AML compliance program.

c. CUSTOMER ACCEPTANCE POLICY

Company Name's Customer Acceptance Policy (CAP) is designed to ensure compliance with legal requirements while aligning with the Company's risk appetite and Business Risk Assessment (BRA). The CAP outlines the criteria for accepting customers, identifies higher-risk individuals, and delineates the necessary Customer Due Diligence (CDD) measures to mitigate risks associated with money laundering (ML), terrorist financing (TF), and proliferation financing (PF).

i. PROHIBITED CATEGORIES OF CUSTOMERS

The Company will not accept customers who fall into the following categories:

- Individuals under the age of 18.
- Individuals listed on sanctions imposed by the UN, EU, or OFAC.
- Individuals with reasonable grounds to suspect involvement in ML, TF, PF, or any other criminal activity.
- Self-excluded customers who are barred from accessing our platforms or included in national self-exclusion registers as required by licensing conditions.
- Individuals who provide documents or information that the Company suspects to be fraudulent or falsified.

ii. RISK INDICATORS

The following risk indicators will be used to categorize customers as low, medium, or high risk:

- **Low Risk:** Customers with stable income sources, consistent transaction patterns, and no red flags.
- **Medium Risk:** Customers with occasional irregularities in income or spending patterns, but no clear indications of criminal activity.
- **High Risk:** Customers with multiple income sources, irregular income streams, high spenders, disproportionate spenders, PEPs, and those using third parties to gamble or exhibiting suspicious behaviors.

iii. CUSTOMER DUE DILIGENCE (CDD) MEASURES

The level of CDD measures will be proportional to the risk classification:

- **Low and Medium Risk:** Simplified Due Diligence procedures will be applied, provided that the customer does not display any risk-enhancing characteristics and transactions remain below the threshold of Cg. 4,000.
- **High Risk:** Enhanced Due Diligence measures will be implemented, which include collecting additional information and documentation. For high-risk customers, ongoing monitoring will be more rigorous, including transaction reviews and alerts for unusual activity.

iv. POLITICALLY EXPOSED PERSONS (PEPS)

The Company implements robust procedures for identifying and managing relationships with PEPs, defined as individuals entrusted with prominent public functions, as well as their close associates and family members.

- **Identification:** Comprehensive screening against reliable databases will be conducted during the onboarding process to determine PEP status.
- **Approval Process:** No business relationship shall be established or continued with a PEP without obtaining senior management approval.
- **Source of Wealth and Funds:** The Company will request a statement from the PEP regarding their source of wealth and verify this information through independent and reliable sources. Additional documentation may be requested if necessary.
- **Enhanced Monitoring:** The Company will conduct enhanced ongoing monitoring of PEPs, analyzing their spending patterns to ensure they align with declared legal sources of funds.

PEP status screening will occur regularly throughout the business relationship. If a customer not identified as a PEP at onboarding later becomes one, the Company will implement enhanced due diligence measures within 30 days. Failure to implement these measures will result in the termination of the relationship with that customer.

v. SANCTIONS SCREENING

The Company is committed to complying with targeted financial sanctions, which require the freezing of funds and assets of individuals and entities identified by the UN and EU as involved in terrorism or proliferation activities.

- **Ongoing Monitoring:** The Company will perform ongoing sanctions screening at key points, including during registration, withdrawal requests, and any changes to personal details or payment methods.
- **Action on True Matches:** If a true match is discovered, the Company will immediately freeze the funds of the affected customer and file a report with the Financial Intelligence Unit (FIU). Services will be terminated upon confirmation of the true match by the supervisory authority, and frozen assets will be held until further instructions are received.

7. CUSTOMER DUE DILIGENCE (CDD)

The Company is required to perform Customer Due Diligence (CDD) under specific circumstances to ensure compliance with Anti-Money Laundering (AML) regulations and to protect the integrity of its operations. The Company must undertake CDD measures when players engage in financial transactions that amount to Cg. 4,000 or more. This includes any deposits or withdrawals made by the player.

In addition to financial transactions, the Company must carry out CDD for any occasional transaction that equals or exceeds Cg. 4,000. Furthermore, if there is any suspicion of money laundering (ML) or terrorist financing (TF), the Company is obligated to conduct CDD. This also applies in situations where there are doubts about the accuracy or completeness of previously obtained identification information from the player.

Financial transactions are defined specifically as deposits and withdrawals; bonuses are excluded from this category. Conversely, wagered amounts and winnings are classified as gambling transactions and do not fall under the definition of financial transactions. To effectively monitor and determine when a player reaches the Cg. 4,000 threshold for CDD purposes, the Company will evaluate not only individual transactions but also any series, combination, or pattern of transactions that exceed this amount. This evaluation will be conducted daily and will include all deposits, withdrawals, and peer-to-peer transfers made by the player.

Additionally, the Company maintains a strict policy against anonymous accounts or accounts held under fictitious names. The Company is committed to identifying each player by collecting their name and other relevant information, which is essential for determining the purpose and nature of the business relationship.

The main responsible department for the Due Diligence process is Factoring and Monitoring (Anti-fraud) Department. In order to perform the due diligence controls, employees use automatic controls, manual reviews and electronic registers.

a. IDENTIFICATION AND VERIFICATION OF THE PLAYER

The Company's CDD procedures require prospective customers to create a full profile at the point of registration. Mandatory information required at the registration stage includes:

- i. Full name;
- ii. Date of birth;
- iii. Permanent residential address;
- iv. Place of birth;
- v. Nationality; and
- vi. Identity number.

To complete the required customer identification and verification process, the Company asks its customers to upload a copy of valid identification documents (passport, identity card, driver's license, or an equivalent document). This request is sent to the customer's registered email address. If the documents are in a different language, the Company will take necessary steps to ensure that the documents adequately prove the customer's identity, such as obtaining a translation of the relevant parts. This may involve asking the customer to submit documents with a certified true translation.

Only documents issued by government agencies that include a photograph are deemed reliable for verifying the customer's identity. Government-issued documents that lack a photograph can be used to confirm the customer's current address, provided the address is included in the document. The Company accepts as proof of permanent residential address copies of utility bills (e.g., electricity, water, gas, telephone landline) or bank statements, as long as they are not older than six months at the time they are received.

b. IDENTIFICATION AND VERIFICATION OF THE BENEFICIAL OWNER

The Company is legally obligated to identify and verify the beneficial owner by confirming that customers are registering accounts to play and transact solely on their own behalf. Furthermore, players must declare that they are not acting on behalf of any third parties. The Company will not solely rely on this declaration. We are committed to actively monitoring player activity to detect any instances where a player may be using the account to play on behalf of others. This ongoing vigilance is essential to maintaining the integrity of our operations and ensuring compliance with AML-TF regulations.

To effectively manage this responsibility, the Company has implemented the following safeguards designed to prevent access to our services by individuals deemed suspicious:

- **Payment Method Verification:** Ensuring that the payment method used for deposits is in the name of the player, insofar as possible.
- **Denial of Service:** Preventing transactions for players attempting to use payment methods not in their own name.
- **Withdrawal Identity Verification:** Confirming the identity of players before processing withdrawals.

8. Understanding the Purpose and Intended Nature of the Business Relationship

While the primary purpose of a gaming account is clear, as part of our CDD measures, the Company must still collect relevant information to develop the customer profile. This involves understanding how a customer generated their net worth. The Company must assess whether this source justifies the projected and actual level of account activity. The extent of information collected must align with the risk rating identified during the Customer Risk Assessment (CRA).

For low- and medium-risk customers, the following measures are deemed sufficient:

- Information from open sources, including social media, can be a supplementary source for understanding a customer's profile.
- Obtaining a declaration from the customer detailing their nature of employment or business, along with their usual annual salary.

For high-risk customers, the following measures must be taken:

- Information provided by the customer must be substantiated by independent and reliable documentation. This could include tax returns, salary slips, or bank statements.
- The Company should collect comprehensive details about the sources of wealth to understand the financial background of high-risk customers.

To analyze and verify this information, the Company may take into account the average national income, average disposable income, and other relevant metrics to gauge expected wagering power based on jurisdiction. This is done in consultation with the risk-based approach, whereby the extent of the mitigation will be based on the identified risks. The customer risk profile developed through this process serves as the foundation for the ongoing monitoring of player activity.

a. TIMELINE FOR COMPLIANCE AND NON-COMPLIANT DOCUMENTS

If the customer cannot provide compliant documents within 30 days from the moment the Cg. 4,000 threshold is reached, the Company shall terminate the relationship with the customer and consider filing an Unusual Activity Report with the FIU, provided that a presumption of ML or TF exists.

During the CDD process, customers may continue to access their accounts while the Company gathers the necessary information. However, if a deposit reaches the Cg. 4,000 threshold, the customer will be prohibited from further deposits or withdrawals, although they may continue to play with their existing balance. Conversely, if the threshold is reached due to a withdrawal request, the account will be completely frozen, halting all gameplay.

If a document submitted by a (potential) customer does not meet the verification standards, the designated staff member must immediately flag it for further examination. The initial review should be thorough to pinpoint the specific reasons for non-compliance. Once a non-compliant document is identified, the customer must be informed without delay.

All actions taken in response to non-compliant documents shall be carefully recorded. This includes the initial identification of the issue, communications with the customer, any escalations, and the final outcome. Comprehensive records should be maintained in the customer's file to ensure a complete audit trail.

b. ENHANCED DUE DILIGENCE (EDD)

The Company shall implement Enhanced Due Diligence (EDD) measures for customers identified as higher risk, with actions tailored to the specific risks identified during the assessment process. These measures aim to intensify monitoring of the business relationship to detect any unusual or suspicious transactions or activities. EDD is required in situations where the risk of ML, TF, or PF is heightened.

In any case, the following scenarios are subject to EDD:

- Residents of high-risk geographic areas: Customers residing in jurisdictions associated with higher levels of corruption or inadequate AML, CTF, and CPF regulations.
- Politically Exposed Persons (PEPs): Individuals who hold prominent public positions or are closely connected to such individuals, which may elevate the risk of corruption.
- Anonymity-favoring products or transactions: Services or products that allow for a higher degree of anonymity, potentially facilitating illicit activities.
- New products and business practices: The introduction of new services, technologies, or delivery mechanisms that may present unforeseen risks.

The measures applied during EDD must align with the identified risks and may include, but are not limited to:

- **Additional Customer Information:** Collect comprehensive information about the customer, including occupation, previous addresses, and relevant data from public databases and online resources.
- **Clarification of Business Relationship Intent:** Obtain further information regarding the intended nature of the business relationship to better understand the customer's gaming habits and expectations.
- **Source of Funds and Wealth (SOF/SOW):** Gather detailed information on the source of funds or wealth for the player. In higher-risk situations, the Company will periodically request SOF information, even if there has been no change in the customer's activity pattern. This ongoing diligence is essential for proactively addressing any potential concerns.
- **Transaction Purpose:** Ask for information regarding the reasons for intended or performed transactions to ascertain their legitimacy and ensure they align with the customer's profile.
- **Senior Management Approval:** Require approval from senior management before commencing or continuing the business relationship with higher-risk customers.
- **Enhanced Monitoring:** Implement increased scrutiny of the business relationship, which may involve more frequent reviews of transactions and account activities.
- **Account Verification for Initial Payments:** Require that the initial payment is made through an account in the customer's name with a bank that adheres to similar CDD standards.

c. TARGETED FINANCIAL SANCTIONS

The Company is committed to complying with targeted financial sanctions, which require the freezing of funds and assets of individuals and entities identified by the United Nations (UN) and European Union (EU) as being involved in terrorism or

proliferation activities. Mechanisms are established to ensure compliance with the Company's legal obligations. This includes, but is not limited to, the following:

- The Company shall comply with relevant sanctions decrees and regulations and monitor any and all amendments thereof and implement these without undue delay.
- The Company shall perform ongoing sanctions screening on customers and also conduct trigger-based sanctions screening of customers at least in the following scenarios:
- At the moment of registration;
- At the moment of withdrawal request;
- At the moment of any request for changes to personal details or payment methods.

In the event that a true match is discovered and confirmed, the Company must immediately proceed with freezing the funds of the particular customer(s), in accordance with the Sanctions Ordinance, and must immediately file a report with the Financial Intelligence Unit (FIU). Once the true match is confirmed by the supervisory authority, the Company shall terminate services and keep the frozen assets until further instruction from the supervisory authority, or otherwise, in light of tipping-off considerations, follow instructions from the supervisory authority.

9. MONITORING

a. MONITORING OF THE ACCOUNT ACTIVITIES

This component is central to the Company's AML&TF efforts. Account monitoring is conducted on the ongoing basis by the officers responsible for various operating aspects of the business. The deposit and withdrawal policies are enforced personally by CFO and Compliance Officer. This enforcement is conducted daily and supported by various thresholds set up to flag the potential problems. Operating Control Matrix describes the controlling processes in detail (Appendix A).

Overall, monitoring of account activities consists of:

- Monitoring of new registrations
- Monitoring of deposit activity
- Monitoring of gambling activity
- Monitoring of account access
- Monitoring of account detail changes
- Monitoring of withdrawal activity
- Monitoring of registration data to ensure it is kept up to date

Critical controlling measures with respect to ML&TF prevention are:

- denial of withdrawals for the inactive funds
- detection of the unusual payment patterns (i.e. deposit activity does not match the betting activity or large deposit movements unwarranted by the betting patterns)
- periodic screening of e-wallets used by the players
- pro-active recognition and prevention of players' fraudulent intentions or activities. This component is an indirect indication of probable ML&TF threats.

The Company's accounting system traces the account movements by individual IP address of the players. List of IP addresses is stored and can be viewed for each game account; all IP addresses are also stored in the logs of the program (including archived). The system has a viewing facility for analysis of a list of players and the number of movements at the specified IP address. Recording of IP addresses allows to track down fraudsters whose activities are connected with gaining access to other customers' player account or gaining possession of their funds (an example of indication to a possible theft of credit card: if BIN code of a credit card used by a player is Cyprus-originated and the IP address of the gaming account is identified as Nigerian. If such a combination occurs, the account is immediately blocked until the owner passes the full verification.

b. TRANSACTIONS MONITORING

Transaction monitoring is a critical component of account activity oversight within the Company, aimed at identifying and preventing unusual transactions that may indicate money laundering (ML) or terrorist financing (TF) threats. This process is outlined in detail in the Operating Control Matrix and involves several safeguards and triggers.

Key Safeguards

1. Monetary Limits: Implementation of absolute monetary limits to control transaction sizes.
2. Single-Player Rules: Policies ensuring one player per account and session, and restrictions on the use of a single currency.
3. Event Bets Monitoring: Specific rules regarding obscure event bets, as detailed in the Operating Control Matrix.

Player Status Assignments

Players are assigned a status and corresponding color codes for visual recognition based on their gaming behavior and history:

- **No Status (Uncolored):** New customers who have not completed the verification process. Limits may be based on a governmental database of self-limited individuals from specific countries.
- **Monitored (Green):** Verified players whose gaming activities have been analyzed by the Anti-Fraud Department, with no unusual actions detected.
- **Arbitrage (Yellow-Red):** Players with a history of placing sure bets.
- **Scammers (Black):** Players identified as engaging in fraudulent activities.
- **Foreigners (Blue):** Players residing outside the Company's core operational regions.
- **Suspicious (Purple):** Accounts under close monitoring by the Payment and Factoring & Monitoring Departments.
- **Potential VIP Players (Pink):** Players who show potential for high-value betting.
- **Existing VIP Players (Orange):** Players consistently placing bets over 100 EUR. Their transactions receive higher processing priority.

Even players with a "good" status (monitored, arbitrage, VIP) are subject to ongoing monitoring by the Payment Department and the Factoring & Monitoring Department to ensure compliance and detect any suspicious activities. High-risk customers, including suspicious players and scammers, are subject to specific monitoring measures:

Categories of High-Risk Players

1. **Suspicious Actions:** Players whose gaming activity is deemed unusual. Their accounts may be limited to bet amounts of 5-10 EUR or equivalent, and unblocking occurs only upon confirmation from the Anti-Fraud, Payment, or other relevant departments.
2. **Fraudsters:** Players identified as cheating. Their accounts are blocked pending investigation.
3. **Vilochniki:** Players placing bets on outcomes that cannot lose, detected through specific gaming patterns. Their activity may be limited or frozen if their winnings exceed 70% of total winnings.
4. **Knopochniki:** Players betting on matches that have already concluded but are not yet recorded in the system. They may have their betting limits adjusted based on their average bet size.
5. **Politically Exposed Persons (PEPs):** Individuals with prominent public functions, whose transactions are continuously monitored to ensure compliance with Enhanced Due Diligence procedures.

Detection Tools

The Company utilizes various databases for the detection of high-risk players, including:

- **United Bookmakers' Database:** A list of known fraudulent players.

- **Payment Systems Database:** Cross-referencing customer registration information with payment records. The Anti-Fraud and Payment departments rely on this data for reconciliations and to identify blocked individuals.

Investigation and Account Suspension

When suspicious activity is detected, the following procedures are followed:

1. **Account Suspension:** A notification appears on the customer's page, and the Support Team requests additional information or documents for investigation. The customer may still access their account, but funds will remain frozen until the investigation concludes.
2. **Documentation of Investigation Steps:** All investigation steps are recorded in the system. If the investigation resolves favorably, the account will be unblocked. If the customer fails to respond or does not provide sufficient information, the account will remain blocked.

Identification of Problematic Gamblers

Problematic gamblers are identified through three primary methods:

1. **Customer Self-Reporting:** Customers may inform the Support Team of gambling issues via email, chat, or phone, requesting limits or temporary account blocking. The Anti-Fraud Department will implement these requests and notify the customer.
2. **Mathematical Review:** The Anti-Fraud Department monitors gambling patterns. For instance, if a player's losses increase tenfold over three months or double each month over 12 months, they are flagged for further communication.
3. **Support Team Review:** Staff members identify problematic gamblers through interactions. Harassment or compulsive gambling behaviors, such as repeated requests for credit, trigger additional scrutiny.

10. REPORTING UNUSUAL ACTIVITIES AND TRANSACTIONS

The Company is committed to identifying and reporting any unusual activities and transactions, including attempted transactions, to ensure compliance with Anti-Money Laundering (AML) regulations. This section outlines the procedures and responsibilities for recognizing, reporting, and investigating unusual transactions.

Employees must report any unusual activity to the Compliance Officer immediately, but no later than 24 hours after the transaction has been executed. This includes any transactions that raise suspicion or deviate from normal behavior.

Employees must submit an Internal Unusual Activity Report (IUAR) to the Compliance Officer. The format of the internal report on unusual activities and transactions is provided in Appendix C.

If a more in-depth investigation is required, the Compliance Officer may request additional information from relevant departments. This investigation must be completed within ten (10) business days.

The Compliance Officer will assess the information available to determine if it is sufficient to warrant filing an Unusual Transaction Report (UTR) with the Financial Intelligence Unit (FIU).

If the Compliance Officer concludes that the activity is unusual, a report shall be submitted to the FIU regarding any unusual monetary operations or transactions within 48 hours.

a. INDICATORS OF UNUSUAL TRANSACTIONS

The Company observes both objective and subjective indicators to assess whether a customer's transaction is deemed unusual. The following transactions or intended transactions are considered unusual:

1. A transaction reported to law enforcement or judicial authorities in connection with money laundering or terrorism financing.
2. An intended transaction carried out by or for the benefit of any individual, legal entity, or group identified on a sanctions list.
3. A transaction amounting to NAf. 5,000.00 or more, regardless of the payment method, which includes:
 - A cashless transaction in the amount of NAf. 5,000.00 or more.
 - Accepting or releasing a deposit of NAf. 5,000.00 or more at the customer's request.
 - Sale of chips to a customer amounting to NAf. 5,000.00 or more.
 - A cash-out transaction of NAf. 5,000.00 or more.
4. Transactions that may reasonably be presumed to relate to money laundering or terrorist financing.

b. PROHIBITION OF DISCLOSURE

All reports and investigations must be handled with the highest level of confidentiality in accordance with applicable laws and regulations. Unauthorized disclosure of information related to unusual activity reports is strictly prohibited and may lead to legal and disciplinary action.

c. PROTECTION FOR REPORTING EMPLOYEES

The Company has implemented measures to safeguard employees and representatives who report suspicions of money laundering, terrorist financing, and/or financing of proliferation to the FIU. Employees reporting such suspicions are protected from threats or hostile actions by other employees, management, or customers, as well as from adverse or discriminatory employment actions.

11. RECORD-KEEPING

1. A complete history of each player's account transactions starting from the date of account opening and to his latest bet is saved on the computer system. The system keeps the following information (Appendix B contains a sample of the customer account history):
2. Primary customer data (required at the registration stage) and scanned documents. The fullness of the data required in each particular case is driven by the risk triggers described in the Customer Risk Assessment Section of this policy i.e. country of the player, currency selected, e-wallets used and other. If a combination of risk triggers gives rise to a particular concern, the employees of Anti-Fraud Department and Payment and Anti-Fraud Department react according to the set of given circumstances.
3. Comments by the employees of the respective departments concerning each player account. There are fields designated to comments in the program for four departments: Anti-fraud, Payments, VIP Players and Support. Each department provides comments (notes) in their respective fields only and strictly in accordance with their official duties. For example, the VIP Players Department usually provides ranking information of VIP players (ranked by stars: from a "small" VIP player to the largest according to graduation, etc.).
When the comments lose relevance with the passage of time, head of the appropriate department may remove a comment however the log will be kept on record indefinitely.
4. System also keeps records regarding profitability of each gaming account for the entire period of its existence – also utilized as an ML&TF risk trigger.
5. All unusual activities and transactions are recognized and recorded in the system. Concurrent analysis is conducted on each such activity or transaction in accordance with the Company Operating Control Matrix. Upon receipt of the Report on unusual activities and transactions, Compliance Officer decides as to the further course of actions concerning possible reporting of the transactions to authorities and licensing authority.
6. All transactions history of a player including amendments, additions and deletions to the transactions are kept for records for 5 years' period. For data and information, the holding period is 5 years following the date of cancellation of customer relationships. Records are maintained on company servers and instantaneous back-up is performed.
7. The system provides technical facilities for sending the messages to customers; such messages are stored in a special Message Box in the context of each player account, as well as in the logs of the system. Disputes with the player arising in the gaming context are solved operationally by communicating with the customers via Skype, email, chat, or phone. The records of disputes are stored in the system.

12. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

The Casino is fully committed to adhering to all applicable laws and regulations related to Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and sanctions enforcement as established by the jurisdiction of Curacao, aligning with international best practices, including the FATF Recommendations. Compliance with the AML/CTF Policy is mandatory for all employees, officers, agents, and third-party service providers. Non-compliance may expose the organization and individuals to significant legal, regulatory, and reputational risks, including fines or penalties imposed by Curacao's authorities, revocation or suspension of the Casino's gaming license, and potential criminal prosecution for wilful violations.

Additionally, non-compliance can lead to reputational damage, resulting in loss of customer trust, negative media exposure, and strained relationships with financial partners. Operational disruptions may also occur, such as freezing of funds, loss of access to financial systems, and increased scrutiny from regulators.

Employees who violate the AML/CTF Policy may face disciplinary actions, including formal warnings, suspension, or termination for serious or repeated breaches, as well as potential referral to law enforcement. Third-party providers may have their agreements terminated if found non-compliant. All employees must understand and comply with the AML/CTF Policy, participate in mandatory training, and report any unusual behavior or breaches to the Compliance Officer, who will ensure that whistleblower protections are in place.

The Compliance Officer and senior management are responsible for investigating violations, determining appropriate disciplinary actions, and reporting serious breaches to relevant authorities. All enforcement actions are documented and reviewed periodically to improve the compliance program.

Appendices

Appendix A. Operating Control Matrix (Fragment)

Number	Areas	Subareas	Control	Control type (prevention/detection)	Procedures description	When/ how often is performed/ triggers	Responsible department
1	Customers	Customers registration	The new customer must fill in the registration form with identity details, home address, valid email address and confirm that he/she is 18 year old, give T&C consent	prevention	System doesn't allow registration of the players who is not 18 years old and who did not fill all the necessary fields	100% coverage	Compliance department
2	Customers	Customers verification	Document verification per Law must be conducted within 30 days after registration. Company uses 3rd party solutions and public information to confirm the identity of the customer.	prevention	The customer need to provide via e-mail or to upload in his personal cabinet the needed personal documents as it is required in the Company's KYC policy (it is public and can be easily found on the website).	100% coverage	Support Team, Compliance department
3	Customers	Customers verification	Invalid documents detection	detection	If the customer provided invalid the Support team will take all needed efforts to contact the customer and request him to update his/her profile with valid documents	100% coverage	Support Team, Compliance department
4	Customers	Customers acceptance	Host country is monitored (prohibited: USA, Israel, France, Estonia, UK and outlying territories, Italy, Spain, Denmark, the Netherlands, Mohawk Territory of Kahnawae, Lithuania, Greece list updates periodically)	prevention	System doesn't allow registration of the players from the prohibited countries	100% coverage	Compliance department
5	Customers	Customers acceptance	Age of the players is monitored	prevention	System doesn't allow registration of the players under 18 years	100% coverage	Compliance department
6	Customers	Customers acceptance	PEPs identification anda sanction lists check (KYC procedure)	detection	All the players are checked within PEPs and sanction lists. Company uses 3rd party solutions and open-sourced databases with PEP and sanction lists. Company permanently check all existing customers.	100% coverage	Anti-fraud department, Compliance department
7	Customers	Customers acceptance (1st deposit stage)	Only 1 account is allowed for 1 player	prevention	Table of first deposits is daily reviewed within the system - IP addresses are checked through "Search IP" button in the programme - deposits done through 1 wallet	100% coverage	Anti-fraud department
8	Customers	Customers acceptance (1st deposit stage)	Full verification for risky players and full verification of the players where the country requires it	prevention	Additional checks are performed for risky players: - passport copies - photo+passport copies - password sending to the registered address - source of wealth and/or source of funds	Special criteria (risk country, suspicious behaviour, risk amount)	Anti-fraud department
9	Customers	Customers acceptance (1st deposit stage)	Black-lists	prevention	all the players are automatically checked within the Black-lists in each Payment system	100% coverage	Anti-fraud department,
10	Customers	Customers acceptance (1st deposit stage)	PEP-lists check by PSPs	detection	all the players are automatically checked within the PEP-lists in each Payment system	100% coverage	Compliance department
11	Customers	Activation of account	Activation of the player can be done only after his e-mail check (it should be real)	prevention	Automatically generated link is sent to the registered e-mail of the player. The account will not be activated, till the link is followed	100% coverage	Anti-fraud department
12	Customers	Changes of customers' information	Changes in registered players' information are monitored by Anti-fraud department.	prevention	Players are responsible for notification of any data changes. For making changes - the player should write the request from the e-mail, that he registered. If the inconsistent information is identified through the playing activity of the player, the account is blocked according to deposit and withdrawal rules.	100% coverage	Anti-fraud department

Who is doing?	To whom is reported?	Reports, back-ups, further actions
Automatic control	Automatic control	Account is not opened
Support Team, Compliance department	Head of Compliance	Any withdrawal from account cannot be processed without verification of the player's identity, address, age.
Support Team, Compliance department	Head of Compliance	Temporary may be applied limits on withdrawal and game till the valid documents will be provided
Automatic control	Automatic control	Account is not opened
Automatic control	Automatic control	Account is not opened
Automatic control	Head of Anti-fraud Department	Need approval from CEO and Head of Compliance for PEP accounts. Enhanced Due Diligence procedure and enhanced monitoring applied for the PEP's account. For persons under sanctions business relationship cannot be settled.
4-5 persons depending on the playing activity	The account is either blocked or agreed with the Head of the Department for blocking	Operational control, history of each player with comments can be reviewed in the system.
4-5 persons depending on the playing activity	Operational review is done by the Head of the Department	Operational control, history of each player can be reviewed in the system
Automatic control	Automatic control	Account is blocked, notification sent to the player
Automatic control	Head of Payments Department	Restrictions to the account undertaken, request for additional documents sent to the player
Automatic control	Automatic control	Automatic control
4-5 persons depending on the playing activity	Difficult cases are agreed with the Head of department	Correspondence with players

APPENDIX B. SAMPLE OF CUSTOMER TRACK-RECORD

[illegible]

APPENDIX C. REPORT ON UNUSUAL ACTIVITIES AND TRANSACTIONS

Date	Reporting officer	Description of unusual activity or transaction	Area ²	Mitigation measures taken NO / YES – description	Comments	
...	...	...	...	...	...	
...	...	...	...	...	...	
...	...	...	...	...	...	

² Customers / Deposits / Withdrawals / Betting rules / Revenue / ML&TF