



TGI ENTERTAINMENT N.V.

AML & CFT Policy and Guideline



VERSION 3.4

TGI ENTERTAINMENT N.V.

Document Information:

Approval	Board of Directors
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 History:

Date	Version	Summary Changes	Approved by Management
October 13, 2022	2.0	Policy update	
August 7, 2023	3.1	Policy update	
May 20, 2024	3.2	Policy update	
October 21, 2024	3.3	Policy update	
April 10, 2025	3.4	Policy update	Global Related Services BV obo TGI Entertainment NV 28 May 2025 

For any questions regarding this policy, please contact the Compliance Officer Andrija Simic.

Contents

1. Policy Statement.....	4
2. Purpose of Document.....	4
..... Definitions	
.....	5
3.....	5
4. What is Money Laundering and Terrorist Financing.....	7
5. Policy Implementation.....	9
5.1. RESPONSIBILITY OF THE SENIOR MANAGEMENT	9
5.2. COMPLIANCE OFFICER	9
5.3. EMPLOYEES	10
6. Business Risk Assessment.....	11
7. Customer Risk Assessment and Risk Matrix	11
8. Customer Acceptance Policy.....	13
8.1. PROHIBITED CATEGORIES OF CUSTOMERS	13
8.2. CUSTOMER DUE DILIGENCE (CDD) MEASURES.....	13
8.3. SANCTIONS SCREENING.....	14
9. Customer Due Diligence	15
9.1. IDENTIFICATION AND VERIFICATION OF THE PLAYER	15
9.2. IDENTIFICATION AND VERIFICATION OF THE BENEFICIAL OWNER	16
9.3. TIMELINE FOR COMPLIANCE AND NON-COMPLIANT DOCUMENTS	17
9.4. ENHANCED DUE DILIGENCE (EDD)	17
9.5. TARGETED FINANCIAL SANCTIONS	19
9.6. POLITICALLY EXPOSED PERSONS (PEPs).....	19
10. Monitoring	21
11. Reporting of Unusual Transactions	22
11.1. PROHIBITION OF DISCLOSURE	22
11.2. PROTECTION FOR REPORTING EMPLOYEES	22
12. Record-Keeping.....	22
13. AML Compliance Program	24
13.1. Appointment of a Compliance Officer	24
13.2. Employee Due Diligence	24
13.3. Training.....	24

13.4.	Independent AML Audit.....	25
13.5.	Examination by the Gaming Control Board	26
14.	Compliance and Consequences of Non-Compliance	27
15.	Countries and Territories excluded from registration	28
	 ANNEX	
		1
16.	I: FIU REPORTING OF UNUSUAL TRANSACTIONS.....	1
	 ANNEX II	
		2
17.	RISK MATRIX.....	2
	 ANNEX III	
		3
	: INTERNAL UNUSUAL TRANSACTION REPORTING FORM	
		3
18.		3

1. Policy Statement

TGI Entertainment N.V. (hereinafter “**TGI Entertainment**” or the “Company”), is licensed and regulated by Curaçao Gaming Authority (CGA) to offer remote (online) games on the internet. In accordance with the license conditions, The Company has developed a comprehensive Anti-Money Laundering, Counter Terrorism Financing and Counter Proliferation Financing (hereinafter “AML, CTF and CPF”) policy (hereinafter the “Policy”).

As a responsible gaming enterprise operating in Curaçao, TGI Entertainment acknowledges the paramount importance of upholding the integrity of our financial systems and preventing the exploitation of our operations for unlawful activities. Our commitment to compliance transcends mere legal requirements; it is a core component of our corporate responsibility and ethical principles.

The scope of this AML & CFT guideline is to ensure that **TGI Entertainment N.V.** and all its subsidiaries, and staff members are compliant with the regulations & internal procedures to ensure that AML & CFT risks are mitigated and dealt with accordingly. This document is adapted for compliance with the following laws and amendments in the following countries; Curacao, The Republic of Cyprus, and the European Union (EU).

This policy applies to all departments and staff of **TGI Entertainment N.V.** as well as all other supporting departments or third parties assisting **TGI Entertainment N.V.** in obtaining its corporate and financial goals and obligations. This policy will be reviewed whenever there is any relevant change in legislation that might also affect this AML/CFT/KYC policy.

TGI Entertainment N.V.’s general policy is not to accept any players whose funds have been emanated from illicit proceeds or for which there is reason to believe that they have been derived from illicit proceeds. TGI Entertainment N.V. is committed to take adequate measures to safeguard against abuse of its facilities, platform and services for money laundering, financing of terrorism or proliferation purposes.

2. Purpose of Document

The procedures below describe how **TGI Entertainment N.V.** to its best efforts and knowledge adheres to the AML, CFT & KYC requirements applicable to fighting Money Laundering and Terrorism Financing. This procedure also serves as a guideline to all staff members in reminding them of their obligations and personal responsibility of fighting money laundering and terrorism financing.

The purpose of this Policy is to ensure the Company’s compliance with the relevant legal and regulatory requirements from the authorities in charge of the supervision of AML, CTF and CPF

matters for the gaming sector are the CGA and the Curaçao Financial Intelligence Unit (FIU), while simultaneously ensuring the integrity and sustainability of the operations of the Company.

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:

- 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);
- National Ordinance of the 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157);
- 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.

3. 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 the process of concealing the true origins of illegally obtained funds, making them appear to originate from legitimate sources. ML encompasses a broad range of activities, including attempts to turn criminally obtained money into 'clean' money, transferring the benefits of crimes like theft or fraud, and facilitating the laundering of criminal or terrorist property. This process typically occurs in three stages – placement, layering and integration.

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. Unlike ML, which always involves proceeds from illegal activities, terrorist financing may not necessarily derive from illicit sources; instead, it often utilizes legitimate funds from charitable donations, business profits, or foreign government sponsorships. While both terrorism financing and money laundering may employ similar methods – such as cash smuggling, structuring, wire transfers, and the use of debit and credit cards – the primary concern of TF is to obscure the intended use or end recipient of the funds rather than their origin. Additionally, funding for terrorist activities does not always require large sums of money, as it can accumulate over time through simple transactions.

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.

4. What is Money Laundering and Terrorist Financing.

Money Laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal, illegal activities. If undertaken successfully, it allows them to maintain control over those proceeds and, ultimately, to provide a legitimate cover for their source of income. Failure to prevent the laundering of the proceeds of crime, permits criminals to benefit from their actions, thus making crime a more attractive proposition.

The three stages of Money Laundering are the following;

- Placement: illegally-obtained funds are placed into the financial system
- Layering: the funds are moved and ownership is changed (funds are often divided into multiple parts, so-called structuring) to obscure the origin

- Integration: the funds are used to purchase goods and services, invest in businesses or financial services, and are therefore made to look legitimate

A company may be the target of Money Laundering in any of these three stages, therefore at **TGI Entertainment N.V.** staff are trained to understand these stages and money laundering vulnerabilities, in general, to help recognize the threat if being faced with it. Furthermore specific AML training is given to relevant staff members according to their position and responsibilities.

In addition to the money laundering threats imposed by clients or players or third parties, internally staff must be vigilant not to commit any of the following offenses:

- knowingly assisting in concealing, or entering into arrangements for the acquisition, use, and/or possession of, illegally obtained funds,
- failing to report knowledge, suspicion, or where there are reasonable grounds for knowing or suspecting, that another person is engaged in money laundering, financing of terrorism, or that the funds are the proceeds of crime, and,
- tipping off, or prejudicing an investigation

Terrorist Financing is the process of making funds or other assets available to terrorist groups or individual terrorists to support them, even indirectly, in carrying out terrorist activities. Such process in fact comprises two separate types of financial activity:

- money and other assets generated by acts of terrorism; and
- money and other assets intended to fund acts of terrorism (including the promotion of terrorism, and the radicalization of individuals).

The funding of terrorist activity, terrorist organizations, or individual terrorists may take place through funds deriving from legitimate sources or from a combination of lawful and unlawful sources. Indeed, funding from legal sources is a key difference between terrorist organizations and traditional criminal organizations involved in money laundering operations.

Another difference is that while the money launderer moves or conceals criminal proceeds to obscure the link between the crime and the generated funds and avails himself of the profits of crime, the terrorist's ultimate aim is not to generate income from the fund-raising mechanisms but to obtain resources to support terrorist operations.

Although it would seem logical that funding from legitimate sources would not need to be laundered, there is nevertheless often a need for terrorists to obscure or disguise links between the organization or the individual terrorist and the legitimate funding sources. Therefore, terrorists must similarly find ways to process these funds in order to be able to use them without drawing the attention of authorities.

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.

5.1. RESPONSIBILITY OF THE SENIOR MANAGEMENT

The Senior Management is responsible for:

- Set and approve the principles of the AML/CFT Policy.
- Appoint and communicate with the Compliance Officer.
- Define the roles and responsibilities of the Compliance Officers.
- Ensure systems and controls are effective for compliance.
- Provide Compliance Officers with timely access to necessary data (e.g., customer identity, transaction records).
- Ensure all employees know whom to report unusual transactions to.
- Provide adequate resources (staff and technology) for Compliance Officers.
- Assess and approve the annual report, addressing any identified weaknesses or deficiencies.

5.2. COMPLIANCE OFFICER

The Company has appointed senior compliance officer will be designated, separate from our gaming operations, responsible for overseeing the AML program and ensuring compliance with regulations. Our AML/CFT compliance officer will have timely access to customer identification data, transaction records, and other relevant information. This officer will operate independently to ensure robust compliance.

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.

The compliance officer shall be assigned at least the following responsibilities:

- To design and implement the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the casino's policy and procedures;
- To organize training sessions for the staff on various compliance-related issues;
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;

- To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- To keep records of internally and externally reported unusual transactions;
- To execute closer investigation of unusual transactions if necessary;
- To prepare the external report of unusual transactions;
- To make necessary changes to the AML program;
- To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements; and
- To prepare periodic information on the casino's efforts against money laundering and financing of terrorism and financing of proliferation.

5.3. EMPLOYEES

Employees have the following responsibilities:

- Understanding and Compliance: Familiarize themselves with the AML, CTF, and CPF policy, ensuring adherence to all relevant laws and regulations.
- Training Participation: Attend mandatory training sessions on AML regulations and procedures to recognize suspicious activity.
- Customer Identification and Due Diligence: Conduct customer due diligence (CDD) measures, including verifying customer identities and understanding the purpose of transactions.
- Monitoring Transactions: Monitor customer transactions for unusual or suspicious activities and report findings to the Compliance Officer.
- Reporting Obligations: Submit Internal Unusual Activity Reports (IUAR) to the Compliance Officer within 24 hours of identifying suspicious transactions.
- Confidentiality Maintenance: Maintain the confidentiality of all reports and investigations related to unusual activities, avoiding unauthorized disclosures.
- Ongoing Monitoring: Participate in the ongoing monitoring of customer profiles and assess changes that may indicate increased risk.
- Documentation: Accurately document all actions taken in response to suspicious activities and maintain records as required by the policy.
- Cooperation with Compliance Officer: Collaborate with the Compliance Officer during investigations and audits, providing necessary information and access to records.
- Prohibition of Anonymity: Ensure that no anonymous or fictitious accounts are allowed, adhering to the customer acceptance policy.

6. 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.

7. Customer Risk Assessment and Risk Matrix

The Customer Risk Assessment procedure is a critical element of TGI Entertainment N.V.'s internal Anti-Money Laundering (AML) program, aimed at evaluating the specific risks associated with providing services to customers. The assessment initiates at the start of the business relationship when a new player registers for an account. At this stage, a basic risk assessment is conducted based on the information collected during registration, including the player's jurisdiction and results from initial searches and screenings.

Key Assessment Factors:

- **Customer Risk:** The initial risk profile considers various factors, including the player's background, occupation, and transaction patterns. Players who have not yet reached the €2,000 deposit threshold undergo a basic risk evaluation. Once a player reaches the €2,000 level, a more comprehensive risk assessment is conducted. This enhanced assessment incorporates additional information regarding the purpose and intended nature of the business relationship, players' deposit methods, and their overall profiles.
- **Product/Service Risk:** The risk associated with the casino's offerings is evaluated, particularly focusing on products that may allow customers to influence outcomes. Payment methods are scrutinized for higher-risk attributes, such as anonymous payment options and unusual account usage.
- **Geographic Risk:** The geographic location of the player is also taken into account. Players from jurisdictions with weak AML regulations or high levels of corruption are assigned a higher risk rating, referencing resources such as the FATF lists of high-risk jurisdictions.
- **Delivery Channel Risk:** The methods through which customers establish relationships or conduct transactions are assessed. Channels that promote anonymity or non-face-to-face interactions are regarded as higher risk, and reasonable measures will be implemented to mitigate these risks.

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

- **Low-Risk Customers:** For those assessed as low risk, a Simplified Due Diligence process is applied, provided they do not exhibit any risk-enhancing characteristics and their transactions remain below the threshold of €4,000.
- **Medium and High-Risk Customers:** Players categorized as medium or high risk, particularly those who reach €30,000 in total deposits, will require additional scrutiny. Their accounts will be flagged for further analysis to build a more detailed profile. This may include obtaining Enhanced Due Diligence (EDD) reports from third-party providers. If any suspicions arise from the EDD report or account analysis, the source of wealth and supporting documentation may be requested. Conversely, if no suspicions are identified, no further documentation will be needed at that stage.
- **High-Risk Customers:** Upon reaching the applicable pre-established deposit thresholds, customer profiles are automatically elevated to high-risk status, triggering mandatory EDD processes. A second-tier threshold of €100,000 in total deposits necessitates the provision of source of wealth/funds and any additional supporting documentation required to verify the origins of the deposits.

To enhance monitoring capabilities, TGI Entertainment N.V. is also seeking the implementation of an automated risk assessment tool to assist in tracking players' spending behaviors effectively.

Please refer to the Risk Matrix in Annex II.

8. Customer Acceptance Policy

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

8.1. 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.

8.2. CUSTOMER DUE DILIGENCE (CDD) MEASURES

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

Basic CDD: All new users must duly identify themselves by completing the KYC (Know Your Customer) screening upon registration. This includes providing the following information:

- Full name
- Title
- Date of birth
- Residential address

New registrations are reviewed daily, and accounts with falsified or incomplete details are filtered out and blocked. The verification process involves a two-stage check:

Stage 1: A phone call to confirm the registered details of all new depositors.

Stage 2: Submission of ID documentation (proof of ID and proof of address) and bank account verification.

Accounts failing Stage 1 will be blocked and contacted to confirm registered information and provide ID documentation. Accounts that do not complete the verification process must be permanently blocked.

High-Risk CDD: Players categorized as high risk, particularly those with linked accounts or who reach significant deposit thresholds, will undergo Enhanced Due Diligence (EDD). This includes additional scrutiny, collecting further information and documentation, and ongoing monitoring of their transactions.

8.3. 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. New registrations are checked using the Global Identity Verification Services program, Trullio, along with the Refinitiv tool for sanctions screening.

Ongoing Monitoring: The Company conducts 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.

9. Customer Due Diligence

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.

9.1. 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.

9.2. 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.

1. 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.

9.3. 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.

9.4. 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.

9.5. 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.

9.6. POLITICALLY EXPOSED PERSONS (PEPs)

Currently, all players are screened for PEP status. These checks are also carried out on an ongoing basis to ensure that none of the players' PEP status has changed. When dealing with PEPs, the following EDD measures are taken:

- ❖ declaration signed by the client confirming his position or reason for the PEP status
- ❖ approval from senior management
- ❖ declaration of the source of wealth with supportive documentation
- ❖ declaration of the source of funds involved in the business relationship, and

more frequent ongoing monitoring

PEP is defined as a person who has been entrusted with a prominent public function. Examples of such functions are:

- ❖ Heads of State, Heads of Government, Ministers and Deputy and Assistant Ministers, and Parliamentary Secretaries
- ❖ Members of Parliament or similar legislative bodies
- ❖ Members of the governing bodies of political parties
- ❖ Members of the judiciary or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances
- ❖ Members of courts of auditors, Audit Committees, or the boards of central banks
- ❖ Ambassadors, chargé d'affaires, and other high-ranking officers in the armed forces
- ❖ Members of the administrative, management, or boards of State-owned enterprises, and
- ❖ Anyone exercising a function equivalent to those set out above within an institution of the European Union or any other international body.
- ❖ The above list is not an exhaustive list and other persons occupying prominent public functions should be also flagged as PEP.

All measures described will also be applied to family members or to persons which are known to be close associates of a PEP.

10. Monitoring

TGI Entertainment N.V. is required to carry out constant monitoring of the business relationship with its clients/ players. This requirement includes the following two actions:

- ❖ the scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions are consistent with the subject person's knowledge of the customer, his business, and risk profile, including where necessary, the source of funds, and ensuring that the documents, data, or information held by the subject person are kept up to date.
- ❖ Transactions are monitored and when certain events are triggered, the MLRO (Money Laundering Reporting Officer) will investigate the relationship with the user and determine whether enhanced due diligence (EDD) or any other action is needed.
- ❖ Other actions would include monitoring the account closely from a responsible gambling perspective, which is also in line with TGI Entertainment N.V.'s social responsibilities and duty of care obligations for the well-being of its users. Please refer to Annex IV.

11. Reporting of Unusual 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 this Policy.

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.

The indicators for reporting are found in Annex I.

11.1. 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.

11.2. 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.

12. Record-Keeping

The Company retains all necessary records of transactions, both domestic and international, for a minimum of five (5) years to ensure compliance with information requests from regulatory authorities. These records must be detailed enough to allow for the reconstruction of individual transactions, including the amounts and types of currency involved, if applicable, to provide evidence for potential criminal prosecutions.

All records gathered through CDD measures, such as copies of official identification documents, account files, and business correspondence, will be stored for at least five (5) years after the business relationship has ended or after the date of an occasional transaction.

Records shall be stored in a manner that ensures their integrity, confidentiality, and accessibility. Access is restricted to authorized personnel only. Regular backups of electronic records shall be conducted and stored in a separate, secure location to prevent data loss.

After the retention period, records shall be disposed of securely to prevent unauthorized access or disclosure.

When properly ordered to do so by any enactment, rule of law or court order, the Company shall provide a document, customer due diligence information, or enhanced due diligence information and the Company will maintain a register of the documents and information provided and will keep a copy of the same.

13. AML Compliance Program

13.1. Appointment of a Compliance Officer

A senior compliance officer will be designated, separate from our gaming operations, responsible for overseeing the AML program and ensuring compliance with regulations. Our AML compliance officer will have timely access to customer identification data, transaction records, and other relevant information. This officer will operate independently to ensure robust compliance.

13.2. Employee Due Diligence

Employee due diligence is a process employed to screen employees with the objective of identifying and reducing The Company's exposure to the risks associated with money laundering and terrorism financing. These procedures apply not only to the Company's contractual employees, but also to its contractors and subcontractors. The employee due diligence process is informed by The Company's risk assessment and the specific roles within the organization.

Any employee whose position may enable them to facilitate ML or TF must undergo screening. This requirement applies to prospective employees prior to their hiring for such roles, as well as current employees from time to time. Regular updates and re-evaluations are essential for maintaining an effective compliance program against ML, TF and PF.

To screen both current and potential employees, The Company will:

- Identify the individuals;
- Verify their identity;
- Confirm their employment history, such as through references; and
- Determine their suitability for the position and assess whether they pose any risk to the Company.

Positions that may render an employee vulnerable to collusion with or coercion by criminal organizations should undergo more rigorous checks. The Company must evaluate whether:

- The employee has a criminal record, which may be verified through a police check.
- The employee is or has been subject to regulatory, court, or legal actions.
- The employee has leveraged bankruptcy laws for personal gain.

13.3. Training

In delivering AML, CTF and CPF training to the designated categories of employees, the Company will consider the necessary knowledge and qualifications required for their duties, responsibilities, and authorizations. As part of the training framework, the Company will outline the AML, CTF and CPF requirements and provide comprehensive information on the measures and activities that staff are expected to undertake within their roles.

The Company will ensure that documentation of the training provided to staff is maintained, capturing the following information:

- Details on the content of the training programs;
- The names of the staff members who have received the training;
- The date on which the training was provided;
- The results of any testing carried out to measure staff understanding of money laundering and terrorist financing requirements; and
- An ongoing training plan.

The Company will regularly update the training programs to reflect any changes in internal and external regulations, as well as developments in the availability of training programs in the market for external training. Furthermore, extraordinary training in AML, CTF and CPF matters will be provided in specific situations, including:

- The introduction of new internal and external regulations related to AML, CTF and CPF that apply to the Company's staff.
- The launch of new products or services that alter the AML, CTF and CPF risk exposure.
- Instances where an employee breaches internal or external AML, CTF and CPF regulations due to a lack of knowledge during the performance of their duties.

13.4. Independent AML Audit

The Company is obligated to conduct an annual independent audit of its Anti-Money Laundering (AML) program, carried out by an independent and qualified third-party auditor. This audit function ensures that the evaluation of the AML program is objective and thorough, with all findings documented appropriately.

The independent audit must include several key assessments, including but not limited to:

Reviewing the Company's AML, Counter-Terrorism Financing (CTF), and Proliferation Financing (CPF) manuals.

Examining customer files to ensure compliance with established policies.

Evaluating the effectiveness of compliance management systems.

Conducting transaction testing to identify any irregularities.

Assessing the adequacy and effectiveness of employee training programs.

Ensuring compliance with all relevant laws and regulations.

Evaluating the system's capacity to detect unusual activities effectively.

Interviewing employees involved in transactions and their supervisors to gather insights on processes.

Sampling unusual transactions and reviewing compliance with both internal and external policies and reporting requirements.

Assessing the effectiveness of the record retention system.

The audit will also evaluate the Company's responsiveness to findings from previous audits. All testing scopes and results will be meticulously documented, and any deficiencies identified will be reported to senior management, accompanied by requests for prompt corrective actions.

By implementing this annual independent audit, the Company reinforces its commitment to maintaining a robust AML program and ensuring compliance with regulatory standards.

13.5. Examination by the Gaming Control Board

The Company shall provide information and documentation related to its money laundering and terrorist financing policies and procedures to GCB examiners during examinations or upon request. The following items must always be readily available:

- The written and approved AML Compliance Program addressing ML/TF/PF.
- Records of the Business Risk Assessment.
- The name and job description of the Compliance Officer responsible for AML policies.
- Records of reported unusual transactions.
- Records of unusual transactions requiring further investigation.
- Records of frozen accounts.
- A schedule of training provided to personnel on ML/TF/PF.
- Assessment reports on the company's AML, CTF, and CPF policies from internal or external auditors.
- Customer files, including risk assessments, CDD, customer acceptance, and transaction information.

14. 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.

15. Countries and Territories excluded from registration

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

- | | |
|------------------------------------|------------------------------------|
| 1. Afghanistan | 40. Ivory Coast |
| 2. Albania | 41. Jordan |
| 3. American Samoa | 42. Lebanon |
| 4. Aruba | 43. Libya |
| 5. Australia | 44. Lithuania |
| 6. Austria | 45. Kuwait |
| 7. Barbados | 46. Malaysia |
| 8. Belize | 47. The Marshall Islands |
| 9. Belgium | 48. Martinique (.FR) |
| 10. Bonaire | 49. The Maldives |
| 11. Bosnia and Herzegovina | 50. Mali |
| 12. Burma/Myanmar | 51. Mozambique |
| 13. Burkina Faso | 52. Myanmar |
| 14. Burundi | 53. The Netherlands |
| 15. The Central African Republic | 54. Nigeria |
| 16. Cameroon | 55. North Korea (Democratic |
| 17. Cayman Islands | People's Republic of Korea) |
| 18. Croatia | 56. Occupied Palestinian Territory |
| 19. Curaçao | 57. Philippines |
| 20. Denmark | 58. Poland |
| 21. The Democratic Republic of the | 59. Puerto Rico |
| Congo | 60. Qatar |
| 22. Egypt | 61. Reunion |
| 23. Eritrea | 62. Republic of Guinea |
| 24. Estonia | 63. Republic of Guinea-Bissau |
| 25. France | 64. Russian Federation |
| 26. French Guyana | 65. Saba |
| 27. Germany | 66. Saint Barthelemy |
| 28. Gibraltar | 67. Saint Martin |
| 29. Greece | 68. Saint Pierre and Miquelon |
| 30. Greenland | 69. Senegal |
| 31. Guadeloupe | 70. Singapore |
| 32. Guam | 71. St. Maarten |
| 33. Haiti | 72. Spain |
| 34. Holy See (Vatican City) | 73. South Africa |
| 35. Italy | 74. Somalia |
| 36. Iran (human rights) | 75. South Africa |
| 37. Iran (nuclear proliferation) | 76. South Sudan |
| 38. Iraq | 77. St. Eustatius |
| 39. ISIL and Al-Qaida | |

- | | | | |
|-----|---------------------------|-----|----------|
| 78. | Sudan | 89. | Vietnam |
| 79. | Sweden | 90. | Yemen |
| 80. | Syria | 91. | Zimbabwe |
| 81. | Tanzania | 92. | Ukraine |
| 82. | Tunisia | 93. | Belarus |
| 83. | Turkey | 94. | Myanmar |
| 84. | United Arab Emirates | 95. | Yemen |
| 85. | USA | 96. | Panama |
| 86. | US Minor Outlying Islands | 97. | Jamaica |
| 87. | US Virgin Islands | 98. | Uganda |
| 88. | Venezuela | | |

16. ANNEX I: FIU REPORTING OF UNUSUAL TRANSACTIONS

For all indicators, the following apply:

- ❖ reporting mandatory of transactions or intended transactions;
- ❖ for all amounts mentioned the following threshold applies: 5,000 ANG or the equivalent thereof in foreign currency USD 2,800 or EUR 2,400

Providers of internet gaming and gambling

Objective indicators

<i>A. A transaction which is reported to the police or judicial authorities</i>	
Indicator	Definition
G0000111	A transaction which is reported to the police or judicial authorities in connection with money laundering or the financing or terrorism.
<i>B. An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance.</i>	
G0000114	An intended transaction carried out by or for the benefit of a person, legal person, group or entity that is mentioned on a list compiled in pursuance of the Sanctions National Ordinance.
<i>C. A transaction amounting to NAF (ANG) 5,000.00 or more, regardless whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner; This comprises in any case the following situations:</i>	
G0000135	1. <i>A giro-based transaction amounting to NAF (ANG) 5,000.00 or more:</i> A giro-based transaction is a transfer from a bank account of the service provider to a local or international bank account carried out at the request of the client addressed to the service provider.
	2. <i>The taking into deposit or the releasing out of deposit of an amount of NAF(ANG) 5,000.00 or more, at the request of the client.</i>
	3. <i>Sale of tokens to a client in the amount of NAF (ANG) 5,000.00 or more.</i> The term "tokens" includes at least chips and credits.
	4. <i>Payout of prizes in the amount of NAF (ANG) 5.000,-- or more.</i>
	5. <i>All other cases.</i>
NB In case of Indicator G0000135: please also indicate the applicable sub-indicator (1,2,3,4 or 5) when reporting a transaction. In case of sub-indicator 5, please always provide a description of the situation.	

Subjective indicator

<i>Suspected money laundering transactions or financing of terrorism.</i>	
Indicator	Definition
G0000211	A transaction giving cause to assume that it may be connected with money laundering or terrorist financing.

17. ANNEX II RISK MATRIX

Risk Matrix LOW	MEDIUM	HIGH	NOT ACCEPTED BUSINESS
players / clients with a satisfactory steady business relationship or history	All activities in between Low and High	Players / clients appearing as PEP individuals	Players / Clients from which there is an indication they might be involved in illicit business
Players / clients that meet all the required KYC standards	All activities in between Low and High	Players/ clients missing KYC information or that stall the process of collecting KYC information	Players/ Clients that don't want to disclose their Source of Funds or Source of Wealth
Players / clients that remain within the set thresholds for a consecutive amount of time	All activities in between Low and High	Players/ clients exceeding maximum threshold	Players/ Clients that don't want to provide the required documents at onboarding or that Stall the process of onboarding
Players / clients that does not raise alerts or red flags	All activities in between Low and High	Players / Clients that raise alerts or red flags	Players / Clients who are not registered to play
Players / clients of which their source of funds is known	All activities in between Low and High	Players / clients of which their profile has changed drastically	Players /Clients appearing on sanctioned lists / watch lists
			players / clients that wants to open multiple accounts
Players/ clients that are registered in a country that is regulated / low risk country	All activities in between Low and High	Players / clients of which their country status has changed to high risk	Players/ Clients younger than 18 years of age
			Players / clients that want to operate in cash

18. ANNEX III: INTERNAL UNUSUAL TRANSACTION REPORTING FORM

Time: _____ Date: _____

Location: _____

Name of Reporter: _____

Reporting No: _____

Player's Transaction information

Kind of Transaction: _____

Transaction amount: _____

Player Information

Player Identification

Last name: _____

Type: ID ☐ Driving license ☐ Passport ☐

First name: _____

Number: _____

Birthday: _____

Date issued: _____

Nationality: _____

Place issued: _____

Gender: ☐ Male ☐ Female

Country issued: _____

Threshold Objective Indicators

☐ Transactions above USD 2800 equivalent EUR 2400

☐ Subjective indicator:

☐ Identification problems with the player

☐ Player did not want to give additional information, but finally did

☐ Player's gambling behavior is atypical for client (player is exceeding thresholds or deposits maximum)

☐ Player is controlled by another person / player

☐ Player does not cash out gains / accumulate gains

☐ Other reason, namely: _____

FIU - INTERNAL REPORTER FORM

Describe Situation:
