

INTERNAL AML PROCEDURE OF ONLINE BETTING COMPANY/ONLINE CASINO

SECTION 1. INTRODUCTION

1.1. BLACKBELT N.V. registration number 162196, a company organized and existing under the laws of Curacao, whose registered office is at Zuikertuintjeweg Z/N, Curacao, (hereinafter — «Company») has experience in securing gaming businesses against criminal misuse and implementing wide-ranging anti-fraud and anti-money laundering processes, procedures, and extensive staff training programs. The company has experience in securing gaming businesses against criminal misuse and implementing wide-ranging anti-fraud and anti-money laundering processes, procedures, and extensive staff training programs.

1.2. The Company is not a financial institution and thus should not be treated as such. A client's account will not bear any interest. The Company is not an exchange and therefore does not execute any conversion between any currencies. For the execution of the payment functions under the agency agreement, the Company coordinates its actions and policies with the principal or the gaming operator (hereinafter — «Operator») and acts on behalf of the Operator to fulfill the payment obligations with customers and businesses.

1.3. Underpinning programs will be knowledge of the Proceeds of Crime Act and Money Laundering indicators usually detected in a gaming environment, particularly in a Card Not Present transactional environment.

1.4. The Company is fully aware of all aspects of the Proceeds of Crime Act and its responsibilities and is well placed to impart knowledge of Anti—Money Laundering measures and requirements having secured major remote and non-remote gaming businesses in this field.

SECTION 2. ANTI-MONEY LAUNDERING AND TRANSACTION FRAUD

2.1. Gaming environments are often targeted by those wishing to launder money. The speed of transactions and the use of multiple payment processing options make gaming businesses especially vulnerable to this activity.

2.2. As a result, many of the initial trading and procedural decisions are either directly aimed at combating this threat, or protections are enhanced as a by-product of the overall commercial and trading approach/strategy taken by the business.

2.3. ALL staff will be given training in Money Laundering indicators such as (but not limited to):

- Unusual Betting Patterns;
- Suspicious deposit and withdrawal patterns (size and frequency);
- Reliability of Card Data;
- Customer verification issues and Identity Theft;
- Account linkage/multiple accounting;

2.4. All instances of suspected Money Laundering attempts must be reported to the MLRO but that suspicion must not be conveyed to the customer and further actions must await consent. The MLRO is then responsible for liaising with, submitting Suspicious Activity Reports. He will also ensure that appropriate registers are kept for all related reporting.

SECTION 3. SECURITY AND MONITORING

3.1 . It is essential to implement adequate monitoring procedures in any gaming business across premises, equipment, people, communications, and transactions. The Company will implement a range of measures and procedures to ensure security and safety in these areas.

3.2. The Company has installed Call recording technology. This has multiple benefits that include:

- Staff Training;
- Ensuring accuracy of bet (timing and placement) and transaction data;
- Customer and Brand Reputation Protection;
- Implementation of robust and frequent monitoring procedures that will guard against and deter collusion between staff and customers;

3.3. The protection of data and the security of software and hardware generally are of prime concern for any business where transactions and data are recorded in a Non-Face to Face environment. Consequently, the Company will implement an overarching policy of 'Encrypt whatever can be Encrypted'. Access to Shared Drives will be strictly limited and monitored and where appropriate, password protected. Data Storage and Back-Up solutions/procedures exist to ensure that Customer Data is not accessible to outside parties and reliably prevents loss of data.

SECTION 4. RESPONSIBLE RELATIONSHIPS WITH CUSTOMERS AND BUSINESSES

4.1. The published policies will make specific reference to fraudulent activity, prior knowledge of a result of the likely result of an event, and matters relating to match-fixing and suspicious events. It will detail the actions we may take where cheating is suspected or identified and will detail the extent to which we will co-operate with regulators and sports governing bodies to tackle these matters. This will in general allow a transparent communication process with customers in these instances.

4.2. However, the Company is acknowledged that if serious criminal activity is suspected or identified, it is also incumbent on them and staff that those suspected of this activity are not 'tipped off' as to those suspicions and subsequent investigations and that in some instances, alternative approaches will be required. Appropriate staff training and escalation procedures will be in place.

4.3. The Company will take all necessary measures to ensure the propriety of its relationships with other businesses. This will entail a standardized due diligence approach often accompanied by Non-Disclosure Agreements where appropriate. This will require default disclosure of ownership and management structures, company incorporation details, address, and contact details. Details of these investigations will be templated, and records kept.

SECTION 5. AML RULES OF THE ACCOUNT USE

5.1 . In order to be able to use the website, a client must first register and open an account.

5.2. One client can open only one (1) account. Only one account for each household, IP, PC is allowed. If a client attempts to open more than one account, all accounts may be blocked or closed and any bets may be voided. Also, any returns, deposits, winnings, or bonuses which a client has gained or accrued during such time as the duplicate account was active will be forfeited by a client and maybe reclaimed by us, and a client will return to the Company on demand any such funds which have been withdrawn from the duplicate account. If a client wishes to open another account, a client may do so by contacting support of the Operator. If a new account is opened, the old account will be closed.

5.3. For transaction security, the Company uses SSL encryption. All customer data will be treated as confidential and will not be sold to third parties.

5.4. A client is not allowed to transfer funds from his/her account to other players or to receive funds from other players into the client's account, or to transfer, sell and/or acquire user accounts.

5.5. The Company reserves the right to retain payments if suspicion or evidence exists of manipulation of the casino system. Criminal charges will be brought against any user or any other person(s), who has/have manipulated the casino system or attempted to do so. The Operator reserves the right to terminate and/or change any games or events being offered on the website.

SECTION 6. FINANCIAL CONTROL

6.1. A client may only participate in games if they have sufficient funds on account for such participation.

6.2. Deposited amounts are available on the account within a reasonable amount of time after the confirmation of the deposit. Before a withdrawal can be made, all previous deposits need to be confirmed.

6.3. A client may only use your own personal credit/debit card or another payment method to fund his/her account. The name appearing on the credit cards, or registered on the payment accounts used for deposits or payouts must correspond to the name registered on the account.

6.4. Cardholders' responsibility is to know the laws concerning online gambling in their country of domicile.

6.5. Participation of minors in the activity offered on this website is prohibited.

6.6. For the execution of the Company's payment functions the Operator reserves the right to carry out verification procedures for each client at first withdrawal. Such verifications may for example include copies of a player's passport, national Identity Card, copies of a player's utility bills, and/or copies of the debit/credit cards used to deposit.

6.7. It's the responsibility of the player to ensure that all documents as a part of the KYC process are genuine. Faked or fraudulent documents provided may result in a confiscation of deposits and potential winnings of the player.

6.8. To make a withdrawal, a player must play through active deposited amounts at least once before the withdrawal. This procedure is in line with anti-money laundering practices.

6.9. The Operator reserves the right to use additional procedures and means to verify a client's identity (Know Your Client) When effecting deposits into the account. This could include (but is not limited to) a selfie with a document or form of identification. To verify a player's account casino management require documents (ID, payment systems, utility bills etc.) in Latin or Cyrillic alphabet. In case the player doesn't have an opportunity to provide documents in the above-mentioned alphabets casino reserves the right to demand video verification where the player shows his/her documents.

6.10. The Operator reserves the right to make a phone call to the number provided in the client's account, which can be a necessary part of the KYC procedure. Until the account is fully verified, no payouts will be processed.

SECTION 7. ANTI-FRAUD POLICY

7.1. If the player is suspected of fraudulent actions including, but not limited to participating in any type of collusion with other players' fraudulent actions against other online casinos or payment provider' chargeback transactions with a credit card or denial of some payments made creating two or more accounts other types of cheating or becomes bankrupt in the country of their residence, the Operator reserves the right to terminate such account and the Company suspends all payouts to the player. This decision is at the sole discretion of the Operator and the player will not be notified or informed about the reasons for such actions.

7.2. Should the Operator become aware of any user who has accepted the bonus or a promotion with the sole purpose of creating a positive expected value on bonus return by using known practices aimed at securing a payout of said bonus by Company or at any way try to take advantage of bonuses received by Operator, then the immediate confiscation of winnings and closure of the account with the right to withhold any further withdrawals will be enforced. An example of advantage play would be delaying any game round in any game, including free spins features and bonus features, to a later time when a client has no more wagering requirement and/or performing new deposit(s) while having free spins features or bonus features still available in a game, the Company reserves the right to withhold any withdrawals and/or confiscate all winnings.

SECTION 8. MONEY LAUNDERING CONTROLS

8.1. In addition, the Company has developed an agreed set of internal procedures about anti-money laundering include:

- Identifying their customers (including their age) and checking their information in detail;
- For protection against identity theft, confidential customer information submitted at any point in time shall be protected from unauthorized or unnecessary disclosure;
- Customer credit card numbers stored on the system shall be secured from unauthorized use;
- Making use of the watch lists containing known or suspected members of terrorist organizations, to try to ensure that they do not hold accounts;
- Monitoring the gaming and in-payment/pay-out behavior of customers;
- Limiting deposits (to a variable extent, since some firms do not have limits but rather monitor carefully those few gamblers who make large online deposits);
- Prohibiting direct payments between customers;
- Prohibiting cash payments;
- Automatic blocking of payments from countries that are not the same as the registered home country of the customer
- After identifying an attempt to launder money, reporting the information to the Financial Intelligence Unit and — depending on the jurisdiction and 'tipping off' rules — blocking the account/ending the commercial relationship.

SECTION 9. POLITICALLY EXPOSED PERSON IDENTIFICATION

9.1 "Politically Exposed Person" means a natural person who is or who has been entrusted with prominent public functions in the Republic or in another country, an immediate close relative of such person as well as a person known to be a close associate of such person:

- (a) heads of State, heads of government, ministers and deputy or assistant ministers;
- (b) members of parliament or of similar legislative bodies;
- (c) members of the governing bodies of political parties;

(d) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;

(e) members of courts of auditors or of the boards of central banks;

(f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;

(g) members of the administrative, management or supervisory bodies of State-owned enterprises;

(h) directors, deputy directors and members of the board or equivalent function of an international organisation;

(i) mayor.

Provided further that no public function referred to in points (a) to (i) shall be understood as covering middle-ranking or more junior officials; Provided furthermore that 'close relatives of a politically exposed person' includes the following:

(a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;

(b) the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;

(c) the parents of a politically exposed person;

9.2. In a situation where an economic or professional transaction or a participant in the performance of an official act, the customer or their actual beneficial owner is a politically exposed person of national level, a member of the family of a politically exposed person of national level, or a person who is a close associate of a politically exposed person of national level, then the obliged person applies the following customer due diligence measures:

A. receives approval from senior management to establish a partnership or to continue business relationships with that person;

B. applies methods of customer due diligence measures to establish the origin of the material wealth and the sources of funds that are used in partnerships or that are used for the transaction;

C. monitors these partnerships in an enhanced manner of customer due diligence and conducts regular enhanced monitoring, except cases specified in legal acts.

9.3. If a politically exposed person of state-level no longer fulfills the public duties entrusted to him or her, then the obliged entity, for at least 12 months, must take into account the risks that have been associated with the person in question and apply the necessary and risk-based methods until it is sure that the risks inherent in a politically exposed person of a national level no longer arise.

9.4. The Company entity may not apply the methods of customer due diligence described in

this part to a politically exposed person of national level, to members of his or her family, and to persons who are considered his or her close associates, if no other circumstances are indicating the presence of other, higher than usual risks.

9.5. The Company should establish the internal procedural rules based on which the decision shall be made whether the potential customer or the actual beneficial owner of the customer is a politically exposed person of state level, a politically exposed person of the local level of a country which is the contracting state of the European Economic Area Agreement or a third country or who performs or performed the public duties assigned to him or her in international organizations. The Company should establish the close associates of a politically exposed person of state-level and members of his or her family only if their connection with the executor of important public duties is known to the public or when the obliged entity has reason to believe that such a relationship exists.

9.6. The Company must apply the enhanced customer due diligence measures in addition to the necessary methods of customer due diligence with regard to a politically exposed person of state-level including the following methods:

A. require the additional information from the customer, as well as to apply all necessary methods to establish sources of wealth and money that are used to establish business relationships or when conducting a transaction;

B. verify data or make inquiries to the relevant databases or open databases or make inquiries or verify data concerning the customer, or to the appropriate supervisory authorities at the customer's location or on official websites of government agencies. The following data should be checked primarily:

C. a politically exposed person can be identified using the

NameScan database: <https://namescan.io/FreePEPCheck.aspx> HYPERLINK

"<https://namescan.io/FreePEPCheck.aspx>", which has a free access, or in any paid database (for example, Thomson Reuters, WorldCheck and others);

D. while checking a politically exposed person of local level, as well as a politically exposed person of national level, it is necessary to perform an additional check up using Google, and also using local search systems in the country of origin of the customer, by entering the customer's name and date of birth both in Latin letters and using the local language.

9.7. The decision to establish a business relationship with a politically exposed person of national level must be taken by the management board of the Company, the responsible member of the management board or the contact person. If a business relationship is established with the customer that will become later on or later it will become known that he or she or actual beneficial owner has become a politically important person of state level in the understanding of this guidance, then it is necessary to inform the man.

9.8. The Company proceeds with PePs screening of clients once a week.

SECTION 10. PROHIBITED COUNTRIES AND SANCTIONS

10.1. The prohibited country is the third country which, on the basis of the OFAC Sanctions Programs, OFSI Sanctions Programs, United Nations Sanctions, Directive (EU) 2015/849 of the European Parliament and of the Council, that regulates the counteraction to money laundering and the financing of terrorism of the financial system and which amends the Resolution (EU) 648/2012 of the European Parliament and of the Council and recognizes invalid, and the Directive (EU) 2005/60/EU of the European Parliament and of the Council and Commission Directive (EU) 2006/70/EU (EU page 141, 05.06.2015, pages 73-117), section 9 part 2, high-risk countries are listed (Annex 14) on the basis of these adopted acts.

10.2. Prohibited countries are listed in Appendix №1, which is an integral part of this policy. If the Company in the commercial or professional activity in the course of a transaction or in the performance of an official act interacts with the participating entity, with a customer, in whose respect an official action is carried out, or with a customer from a sanctioned third country, then the any activity should be prohibited.

10.3. Sanctions are imposed by the EU, the United Nations and governments and include a range of financial or trading restrictions, such as freezes on the assets of and travel restrictions on nominated individuals, bans on financing of state-owned enterprises, prohibitions on the supply of technical, financial and other assistance and outright prohibitions on trade. In its business activities, the Company has due regard to relevant applicable sanction programs.

10.4. EU Sanctions

The EU imposes sanctions within the framework of the Common Foreign and Security Policy, either on an autonomous EU-basis, typically imposed through Council Regulations that have immediate legal effect in member states, or by implementing binding resolutions of the United Nations Security Council. Sanctions imposed by the EU may target governments of third countries or non-member state entities and individuals, such as terrorist groups and individual terrorists. The EU maintains and publishes lists of targeted countries, entities, groups or individuals (EU Sanctions Lists). New kind of sanctions may prohibit any type of financing or funding of entities under sanctions, including entities that are listed on regulated markets in the EU.

Sanctions requirements imposed by the EU have to be followed by all persons and entities doing business in the EU, including nationals of non-EU countries, and also by EU nationals AML and Sanctions policy Detailed requirements and entities incorporated or constituted under the law of an EU member state when doing business outside the EU.

For more information about these sanctions, see the following European Commission website:

http://ec.europa.eu/external_relations/cfsp/sanctions/index_en.htm

10.5. US Sanctions

In the US, the Office of Foreign Asset Control of the US Treasury Department ("OFAC") administers and enforces US-based economic and trade sanctions programs against targeted foreign countries, terrorists, international narcotics traffickers and those engaged in activities related to the proliferation of weapons of mass destruction and other threats to the national security, foreign policy or economy of the US. These sanctions programs are based on US foreign policy and national security goals, as well as on United Nations and other international mandates.

OFAC also publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. Additionally, OFAC lists individuals, groups and entities, such as terrorists and narcotics traffickers, designated under programs that are not country specific. Collectively, such individuals and companies are called Specially Designated Nationals (“SDNs”) (US Sanction lists). New kind of sanctions prohibit any type of financing or funding of entities under sanctions, including entities that are listed on regulated markets in the EU. OFAC maintains and publishes lists of these targeted countries, entities, groups or individuals, referred to generally as sanctions and SDNs lists. A US person is prohibited by OFAC from engaging in a wide range of transactions with any individual, group, entity or country on these lists. For more information about these sanctions, see the following US Treasury Department website: <http://www.ustreas.gov/offices/enforcement/ofac/>

10.6. UN Sanctions

The UN sanctions list is maintained by UN member states and organizations to eliminate terrorism, weapons proliferation, human rights violations, money laundering, deliberate destabilization of sovereign countries, and drug trafficking, etc. Depending on the situation, sanctions are applied to economic, cultural, trading, or diplomatic relationships with targeted countries.

The United Nations Security Council (UNSC) has primary responsibility for the maintenance of international peace and security. It has 15 members (5 permanent members with veto powers—China, Russia, the US, France, and the UK—and 10 non-permanent members), and each member has one vote. Under the Charter of the United Nations, all member states are obligated to comply with Security Council decisions, including sanctions imposed by the body.

For more information about these sanctions see the following website:

<https://www.un.org/securitycouncil/sanctions/information>

10.7. UK Sanctions

Sanctions are restrictive measures that can be put in place to fulfil a range of purposes. In the UK, these include complying with UN and other international obligations, supporting foreign policy and national security objectives, as well as maintaining international peace and security, and preventing terrorism.

The UK implements a range of sanctions regimes through regulations made under the Sanctions and Anti-Money Laundering Act 2018 (the Sanctions Act). The Sanctions Act provides the main legal basis for the UK to impose, update and lift sanctions.

UK sanctions Regulations made under the Sanctions Act apply in the whole of the UK, including in Northern Ireland. The prohibitions and requirements in these Regulations apply to conduct by UK persons. This includes anyone in the UK (including its territorial waters), UK nationals outside of the UK, and bodies incorporated or constituted under the law of any part of the UK. It is government policy for UK sanctions measures to be given effect in the British Overseas Territories and Crown Dependencies to make sanctions as effective as possible.

HM Treasury implements and enforces financial sanctions, through its Office of Financial Sanctions Implementation (OFSI). OFSI helps to ensure that financial sanctions are properly understood, implemented and enforced in the UK.

Financial sanctions include restrictions on designated persons, such as freezing their financial assets, as well as wider restrictions on investment and financial services.

OFSI helps companies understand their financial sanctions obligations, monitors compliance and assesses suspected breaches. OFSI can also issue licences to allow for an activity that would otherwise be prohibited by financial sanctions regulations, under certain circumstances.

For more information about these sanctions, see the following OFSI website:

<https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation>

10.8. The Company screens clients manually against sanctions lists and has due regard to any linkages with this every day. Such linkages will be considered as a risk factor in determining the appropriate level of customer due diligence to be applied and the Company will not undertake any business activities that are not allowed under sanctions.

SECTION 11. CLIENTS IDENTIFICATION

11.1. Clients' identification is a player verification procedure.

The main aim of it is to ensure that the holder of the account is the real person and the money going into the casino account is his own (and not a result of criminal activity). Also, it helps to know for sure that withdrawals are headed towards legitimate bank account, owned by him and not anyone else. It is required if the player's deposits / payments have reached limits, also if the player's account is suspicious. The player must upload the documents by himself.

List of required documents:

- Photo of ID or passport.
- Photo or screenshot of the payment system.
- Photo or screenshot of the document confirming the current address (not older than 6 months old)
- Selfie with ID.
- Source of wealth/funds (bank statements, tax declaration, etc. not older than 6 months old)
- Selfie with a special note (example: Hello 'casino name') and/or other special conditions (blinking eye, head/hand turning etc.)

11.2. Screening - Sanctions & Politically Exposed Person: sanction lists typically contain those involved with organized crime, financial crime, and terrorism or are blocked for political reasons. The main aim of applying additional scrutiny to customers who are classed as a PEP is to mitigate the risk that the proceeds of bribery and corruption may be laundered, or are assets stripped from their country of origin. While screening the customer attention should be paid to the following:

- match by name and surname (need to consider features of transliteration of name and surname in different countries);
- date of birth (if available);
- gender (male/female);
- primary country;
- appearance.

11.3. Additionally, the obtained information must be checked in open sources (Internet search).

While searching for information in open sources, attention should be paid to the following:

- official sources (e.g. government bodies' websites - for the Minister of Finance this will be the website of the Ministry of Finance);
- social networks (Facebook, LinkedIn, Twitter, etc.);
- other sources, which can help to confirm the PEP status of the customer.

11.4. The decision of classifying a customer as PEP, their family member, or close associate should be based on available data, assessment of this data, rational and analytical thinking, logic, and available official guidelines.

11.5 Risk Assessment - based on geographic location (ID issuing country & residence) / Social Media presence and Other Online Footprints/ I.P (& efforts to mask I.P)

How to verify documents:

- Photo of ID document: all data (name, date of birth, citizenship) should be completely coincide with the data in Player's details tab. The document should be valid, the photo of the holder, date of birth, date of issue/expire are a must. For example, passport, ID, driver's license are suitable for identification.
- Photo or screenshot of the payment system: all data should be completely coincides with the data in Payment systems debts tab. Necessary data for cards - first 6 and last 4 digits, name of card holder (same as in Player's details tab), card validity period should be clearly seen. The player has the right to hide other data. Scanned copies are not accepted as PS verification.
- A photo or a screenshot of a document confirming the current address: the data (name, address + date of issue of the document) should be coincides with the data in Player's details tab. Acceptable documents: utility bill / bank statement / payment for mobile services. A photo of registration details in passport is acceptable for the players from the CIS. The document must be no older than 90 days (3 months).
- Selfie with ID: it should be visible the player holds the ID in his hands, a thorough check for editing / photoshop should be made. Optionally, a selfie with ID + a sheet of paper on which the name of the casino and the current date are written can be requested.
- Proof of wealth: a document confirming the welfare of the player. Refers to the origin of the entire net wealth (i.e. total assets). The information that should be obtained should give an indication as to the volume of wealth the player would reasonably be expected to have and provide a picture of how it was acquired. Such information is possible to gather using online footprints and proof by an Enhanced Source of Wealth Declaration.
- Proof of funds: a document confirming the flow of funds to the payment system. Easier to establish than source of wealth but this should not simply be restricted to knowing from

which bank or financial institution the funds may have been received. The information obtained should be substantive, relevant and be able to establish the fund's origin and the method/circumstances under which the funds were acquired. Source of funds can be obtained by detailed bank statements showing debits and credits as deposits and remitted amounts and to which recipients.

- **Screening - Sanctions & Politically Exposed Person:** a sanction lists typically contain those involved with organised crime, financial crime, terrorism or are blocked due to political reasons. Transacting with persons or entities on the list can bring heavy fines and restrictions. The main aim of applying additional scrutiny to customers who are classed a PEP is to mitigate the risk that the proceeds of bribery and corruption may be laundered, or are assets stripped from their country of origin. While screening the customer in OFAC Sanction List Search, we must pay attention to the following: -match by name and surname (need to consider features of transliteration of name and surname in different countries); date of birth (if available); -gender (male/female); -primary country; -appearance. Additionally, we must check the obtained information in open sources (Internet search). While searching information in open sources, we should pay attention to the: -official sources (e.g. government bodies' websites - for the Minister of Finance this will be the website of the Ministry of Finance); -social networks (Facebook, LinkedIn, Twitter, etc.); other sources, which can help to confirm PEP status of the customer. The decision of classifying a customer as PEP, their family member or close associate should be based on available data, assessment of this data, rational and analytical thinking, logic and available official guidelines.
- **Risk Assessment - based on geographic location (ID issuing country & residence) / Social Media presence and Other Online Footprints/ I.P (& efforts to mask I.P):** the information about the country where the document was issued and the player's place of residence is investigated. Some countries may be associated with an increased risk in the gambling industry or financial crimes. The purpose of having the ability to search for information on the Internet using various online footprints is to focus on adverse news or negative information that may be associated with the player, found across different news sources and social media platforms. Checking for adverse information can reveal links to money laundering, financial fraud, drug trafficking, financial threats, organized crime, financial terrorism, and other crimes. These links pose a serious threat to the reputation of organizations and can lead to legal consequences. Suspicious IP are analysed during standard verification or any other investigation, particularly in cases where an account has been dormant or inactive for a significant period. The analysis focuses on examining the connections between IP addresses used to access the account and their frequent changes. If suspicious links are detected, such as unusual or unexpected combinations of IP addresses, it may indicate potential security breaches or unauthorized access to the account.

SECTION 12. CUSTOMER DUE DILIGENCE

The Company undertakes CDD measures in the following circumstances:

- Players engage in financial transactions equal to or exceeding NAf. 4,000.
- Players carry out occasional transactions exceeding the monetary equivalent of NAf. 4,000, whether as a single transaction or a series of related transactions.
- There is a suspicion of money laundering (ML) or terrorist financing (TF).
- The Company has doubts about the veracity or adequacy of previously obtained customer identification data.

12.1 CDD Measures to Be Taken

Identifying the Customer:

- Verify the customer's identity.

Identifying the Beneficial Owner:

- Take reasonable measures to verify the identity of the beneficial owner.

Understanding the Business Relationship:

- Obtain information on the purpose and intended nature of the business relationship.

Ongoing Due Diligence:

- Conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure transactions are consistent with the institution's knowledge of the customer, business, and risk profile, including, where necessary, the source of funds.

12.2 Timing of CDD Measures:

- CDD measures (1-3) must be completed at the time the NAf. 4,000 threshold is reached.
- Casinos are required to apply a minimum level of CDD measures when entering a business relationship (e.g., opening an account).
- At least personal details must be collected, and sanctions screening must be conducted when opening an account.

- Players may be allowed to use their gaming account while carrying out CDD measures. However, if the NAF. 4,000 threshold is reached, players are not allowed to deposit funds into or withdraw funds from the account.

Additional Measures:

- The threshold must be calculated on a daily basis, taking all deposits and withdrawals into account since the establishment of the business relationship, including peer-to-peer transfers.
- If documentation is not received within 30 days of reaching the threshold, the casino must terminate the business relationship and report the transaction to the Financial Intelligence Unit (FIU) if there is a presumption of ML.
- Conducting CDD at the earliest possible opportunity can limit situations in which ill-gotten funds are received.

12.3 Inability to Complete Customer Due Diligence (CDD)

In instances where the Company is unable to complete the required CDD measures, the following actions must be taken:

Account and Business Relationship Initiation:

- The casino operator must refrain from opening the account, commencing the business relationship, or performing the transaction if CDD requirements cannot be met.

Termination of Existing Business Relationships:

- If a business relationship is already established and the casino operator is unable to complete the necessary CDD measures, the operator must terminate the business relationship promptly.

Reporting Obligations:

- The Company is required to submit an unusual transaction report to the Financial Intelligence Unit (FIU) if there is a presumption of money laundering (ML), terrorist financing (TF), or proliferation financing (PF).

SECTION 13. ENHANCED CUSTOMER DUE DILIGENCE

In circumstances where the risk of money laundering (ML) or terrorist financing (TF) is heightened, enhanced Customer Due Diligence (CDD) measures must be implemented to mitigate the increased risk. Enhanced CDD is required in the following scenarios:

- Politically Exposed Persons (PEPs): This includes both international and domestic PEPs, who pose a higher risk due to their prominent public positions.
- New Technologies: Emerging technologies that may present increased risks due to their anonymity or potential misuse.
- Higher-Risk Countries: Transactions or relationships involving countries known for higher risks of ML or TF.
- Other Higher-Risk Situations: Any other situations that present a heightened risk of ML or TF.

13.1 Enhanced CDD Measures:

In high-risk situations, the Company operator should consider the following enhanced measures to effectively mitigate risk:

Additional Information Collection:

- Obtain further details about the player, such as occupation and volume of assets. This can be achieved through public databases, internet searches, and other available sources.

Frequent Data Updates:

- Regularly update the player's identification data to ensure its accuracy and relevance.

Source of Funds (SoF) and Source of Wealth (SoW):

- Gather information regarding the source of funds or source of wealth of the player to verify legitimacy.

Transaction Information:

- Obtain detailed information on the reasons for intended or performed transactions to assess their legitimacy.

Senior Management Approval:

- Secure approval from senior management before commencing or continuing the business relationship in high-risk cases.

Enhanced Monitoring:

- Conduct more rigorous monitoring of the business relationship by increasing the frequency and depth of controls and examining transaction patterns for unusual activity.

Initial Payment Requirement:

- Require that the first payment be made through an account in the player's name at a bank that adheres to similar CDD standards.

SECTION 14. SIMPLIFIED CUSTOMER DUE DILIGENCE

When the risk of money laundering (ML) or terrorist financing (TF) is assessed to be lower, simplified Customer Due Diligence (CDD) measures may be implemented. These measures are designed to reflect the lower risk and should be proportionate to the nature of the lower risk involved.

14.1 Simplified CDD Measures

In scenarios where simplified CDD is appropriate, the following measures may be considered:

Delayed Verification:

- Verify the identity of the player and the beneficial owner (BO) after the establishment of the business relationship, rather than before.

Reduced Frequency of Updates:

- Implement less frequent updates of customer identification data, recognizing the lower level of risk.

Minimized Ongoing Monitoring:

- Reduce the degree of ongoing monitoring and transaction scrutiny, based on a reasonable monetary threshold that reflects the lower risk profile.

Infer Purpose and Nature:

- Simplify the process of understanding the purpose and intended nature of the business relationship by inferring these aspects from the type of transactions or the nature of the established relationship, rather than requiring extensive specific information.

14.2 Limitations of Simplified CDD

Simplified CDD measures are not permissible in the following situations:

- Suspicion of ML or TF: Simplified measures cannot be applied if there is any suspicion of money laundering or terrorist financing.
- Higher-Risk Scenarios: Simplified CDD is not acceptable in higher-risk scenarios or where there are concerns related to heightened risk factors.

SECTION 15. REPORTING OF UNUSUAL TRANSACTIONS

The Company are required to report unusual transactions or intended transactions to the Financial Intelligence Unit (FIU) to support the prevention and detection of money laundering (ML) and terrorist financing (TF). The reporting procedure is essential for maintaining the integrity of financial operations and ensuring compliance with regulatory standards.

14.1 Definition of Unusual Transactions:

An unusual transaction is defined as a transaction or series of transactions that is inconsistent with the player's known profile. To determine whether a transaction is unusual, both objective and subjective indicators are used.

14.2 Objective Indicators:

Objective indicators of unusual transactions include:

- Transactions reported to police or judicial authorities.
- An intended transaction involving a natural or legal person listed on a UN or EU sanctions list.
- Transactions equal to or exceeding NAf. 5,000, including bank transactions, sales of chips or credits, and payments of prizes.
- Transactions where there is reason to assume possible connections to ML or TF.

14.3 Procedure for Reporting

Submission via goAML Portal:

- Reports must be submitted through the goAML portal at <https://portal.fiucuracao.cw>. Companies must register to gain access to this portal, and all reports should be submitted in English.

Reporting Timeline:

Objective Indicators:

- Reports of transactions that meet objective indicators must be submitted within 48 hours of the transaction occurring.

Subjective Indicators:

- Report internally to the Compliance Officer (CO) within 24 hours.
- The CO has 10 working days to conduct the relevant research.

FIU Reporting: If a presumption of ML or TF exists, the CO must report to the FIU within 48 hours.

Examples of Situations Possibly Related to ML or TF

- Betting Accounts: Setting up multiple betting accounts with deposits just below the reporting threshold, followed by rapid withdrawals.
- Cash Transactions: Regularly depositing or transacting similar amounts of cash, or funding accounts with credit/debit cards, prepaid cards, checks, and cryptocurrency and then requesting payouts.
- Inconsistent Income: Unexplained income that is inconsistent with the player's financial situation or profile.
- Machine Credits: Claiming machine credits or payouts without a corresponding jackpot.
- Multiple Accounts: Associating with multiple accounts under different names.
- Threshold Patterns: Frequent betting transactions or cash deposits/withdrawals just below the reporting threshold.
- Parallel Betting: Betting against associates or intentionally losing to facilitate the receipt of casino-issued checks or wire transfers of legitimate winnings.
- Currency Exchanges: Multiple or unusual currency exchanges, particularly those involving low denomination bills being exchanged for high denomination bills, or exchanges with minimal gambling activity.
- Wire Transfers: Frequent wire transfers or currency exchanges just below thresholds, or 'cash out' transactions without corresponding 'buy in' transactions.

12.1. The Company must retain the following records and information for a period of five years after the end of a business relationship with a client or after the date an occasional transaction was completed:

(a) Copies and information for compliance with the Client Identification process covered in section 11.

(b) Evidence and records of transactions both domestic and international

(c) Correspondence documents with clients

(d) Suspicious Transaction Reports and/or Suspicious Activity Reports performed by staff members including the examination performed by the CO, the corresponding findings and any subsequent communication with FUI Curacao.

(e) Player risk profile

12.2. Records and information retained must be visible, legible and of sufficient content and quality, to permit reconstruction of transactions so as to provide, if needed, evidence for prosecution of criminal activity. It is highlighted that processes should be established, for the retrieval of records and information retained, which must be accessed timely and without due delays. In cases where it is reasonably justified, the Company should retain records and information for five additional years, bringing the total retention period to a maximum of ten years after the end of a business relationship with a client or after the date an occasional transaction was completed. Reasonable justification refers to the prevention, detection and investigation of Money Laundering and Terrorist Financing in relation to ongoing criminal proceedings or suspicions.

SECTION 13. EMPLOYEE TRAINING

13.1. The Company ensures that its employees, agents or other individuals authorized to act on the Company behalf are adequately trained and informed about the requirements set out in the Company policies and procedures. The Company also ensures that the daily duties of its employees are executed in accordance with the Company regulations and technical instructions specified in the Company ANTI-MONEY LAUNDERING POLICY. Any employee, who violates ANTI-MONEY LAUNDERING POLICY regulatory documents or acts illegally in the course of performance of his/her duties, shall be subject to disciplinary sanctions and liability as provided for in the regulatory enactments of Curacao.

13.2. The Company establishes a system of tailored training for its employees (employees, who have contact with clients such as front-line staff or agents; employees who are involved in client transaction activities and handle client's funds; employees who are responsible for implementing or overseeing the compliance program (such as senior management, information technology staff or internal auditors), etc.) so that they understand their obligations under the Regulator, how the Company business or their particular profession could be vulnerable to ML/TPF activities, the Company compliance policies and procedures and their roles in detecting and deterring ML/TPF activities.

13.3. The training program shall include at a minimum:

- ML/TF concepts, definitions of ML/TF, why criminals choose to launder money and how the process for ML/TF usually works;
- the Company compliance policies and procedures for preventing and detecting ML/TF, including reporting, client identification, know-your-client, client due diligence and record keeping obligations;
- Responsibilities of the Company employees, agents or anyone else acting on the Company behalf when dealing with suspicious transactions.

13.4. Compliance training is comprised of two key elements:

Induction training – Compliance Officer is responsible for identifying relevant new staff that is required to undergo induction training within 30 days after commencement of employment relationship. The training is conducted by the AML and Compliance Department and/or Compliance Officer or the Compliance Officer may engage an external service provider. Until a new member of staff has been signed off as competent, no client servicing activities are allowed; Refresh training - all relevant staff must undergo refresh training on a semi-annual basis. The training is conducted by the AML and Compliance Department and/or Compliance Officer or the Compliance Officer may engage an external service provider. Testing of staff's knowledge is carried out after the training.

The company obtains acknowledgement from staff that they have received the necessary training by requesting staff to sign their attendance at training sessions. Overall monitoring of attendance and testing results are recorded manually and stored in an electronic form.

SECTION 14. RISK SCORING

14.1. The Company's assessment of customer risk marks each customer account as falling within a low, medium, high-risk or very high risk category.

As part of our risk assessment policy, we classify potential threats based on various characteristics and operational contexts.

Very High Risk is associated with activities involving unregulated virtual currency exchanges and corporate structures using bearer shares that ensure client anonymity. These risks are exacerbated when services are provided non-face-to-face through intermediaries.

High Risk is characteristic of non-profit organizations sending funds to high-risk jurisdictions, correspondent banks, and fiduciary arrangements. Risks increase with the use of internet-based products or services susceptible to high money laundering and terrorist financing risks, especially when transactions are conducted non-face-to-face with insufficient technological safeguards.

Medium Risk applies to highly paid employees, public figures, and the general public using retail products. This risk may be moderate, particularly when using technological systems with embedded safeguards in non-face-to-face transactions.

Low Risk is observed for pensioners and average-salaried employees using products with limited transaction or deposit thresholds, especially when transactions are conducted face-to-face.

Each risk category is also influenced by the country rating, which considers the broader geopolitical and regulatory environment.

	A	B	C	D	E	F
1	Criteria	TYPE OF CUSTOMER	PRODUCT/SERVICE	IDENTIFICATION	COUNTRY RATING	
2	Choose one	Pensioners, Average-salaried employees	internet based products, Services or products identified as po	Face to face	Germany	Assigned Risk Rating
3	Rating	1	3	1	1	High
4						
5						
6						
7						
8						
9						
10						
11						

	A	B	C	D	E	F
	Criteria	TYPE OF CUSTOMER	PRODUCT/SERVICE	IDENTIFICATION	COUNTRY RATING	
	Choose one	Highly paid employees, Public figures, General public	Retail products	Face to face	Cyprus	Assigned Risk Rating
	Rating	2	2	1	1	Medium

SECTION 15. TRANSACTIONS AND ONGOING MONITORING

15.1. Below are the most common money laundering-related red flags the Company should watch out for:

- Unusual betting patterns with players placing large bets on low-risk games or frequently changing betting patterns.
- Frequent large transactions.
- Rapid deposit and withdrawal cycles with criminals depositing large sums to their accounts and withdrawing them quickly.
- Multiple accounts and IP addresses for conducting transactions

15.2. The Company is committed to implementing thorough Customer Due Diligence (CDD) processes for all transactions. This includes a comprehensive customer verification at the time of account creation, with the collection and validation of necessary identification documents. Transparent transaction records are maintained for each customer, detailing deposits, withdrawals, and gaming activities.

15.3. The Company applies enhanced customer due diligence measures and enhanced ongoing monitoring, in addition to the required CDD measures, to manage and mitigate the money laundering or terrorist financing risks arising in the following cases:

- in any business relationship with a customer situated in a high-risk third country or in relation to any transaction in relation to which the operator is required to apply CDD measures, where either of the parties to the transaction is resident in a high-risk third country

- if the operator has determined that a customer or potential customer is a PEP, or a family member or known close associate of a PEP
- in any case where the operator discovers that a customer has provided false or stolen identification documentation or information and the operator proposes to continue to deal with the customer
- in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose
- in any other case which, by its nature, can present a higher risk of money laundering or terrorist financing.

15.4. In the case of business relationships with customers situated in high-risk third countries or transactions where either of the parties to the transaction are resident in a high-risk third country, the enhanced measures undertaken must include:

- obtaining additional information on the customer
- obtaining information on the source of funds and source of wealth of the customer
- obtaining information on the reasons for the transactions
- conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

15.5. In the case of transactions that are complex or unusually large, or where there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose, the enhanced measures undertaken must include:

- as far as reasonably possible, examining the background and purpose of the transaction
- increasing the degree and nature of monitoring of the business relationship in which the transaction is made, to determine whether the transaction or relationship appear to be suspicious.

15.6. Depending on the requirements of the case, the enhanced measures undertaken in any case may also include, among other things:

- seeking additional independent, reliable sources to verify information provided or made available to the casino operator
- taking additional measures to understand better the background, ownership and financial situation of the customer
- taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship

15.7. When assessing whether there is a high risk of money laundering or terrorist financing in a particular situation, and the extent of the measures which should be taken to manage and mitigate the risk, the Company takes account of the following risk factors, among other things, whether:

- the business relationship is conducted in unusual circumstances
- the customer is resident in a geographical area of high risk
- payments will be received from unknown or unassociated third parties of the customer

15.8. In addition whether the business relationship or transaction involves countries:

- identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter money laundering or terrorist financing
- identified by credible sources as having significant levels of corruption or other criminal activity, such as money laundering, terrorism, and the production and supply of illicit drugs
- subject to sanctions, embargoes or similar measures issued by, for example, the European Union or the United Nations
- providing funding or support for terrorism

15.9. Understanding player behavior is integral to effective ongoing monitoring. The Company utilizes behavioral analytics to establish baseline patterns for individual players and detect deviations that may indicate suspicious activities. By considering factors such as playing habits, deposit and withdrawal frequency, and gaming preferences, unusual trends can be identified and trigger investigations where necessary. Behavioral analytics serve as a method in staying ahead of potential risks associated with money laundering or other illicit activities.

16.0. To further enhance ongoing monitoring, the Company has established predefined thresholds for various transactional parameters. Any transactions or account activities surpassing these thresholds trigger immediate alerts for review. This proactive approach allows to focus attention on high-risk activities promptly, mitigating the potential for financial crimes. Regular reviews of these thresholds are conducted to adapt to changes in the gaming landscape and to ensure that our monitoring efforts remain effective.

16.1. The Company proceeds with the ODD of clients on the following basis:

- Once per month for a High-Risk client and a Very High-Risk client.
- Once per 6 months for a Medium-risk client.
- Once per year for a Low-risk client

List of countries No.1 (countries against which the United Nations, the United States, the UK or the European Union have imposed financial or civil restrictions) for the geographic risk assessment of the Client, the Client's UBO and the Client's partners

No	Country code	Country
1	AF	Afghanistan
2	BA	Bosnia and Herzegovina
3	BI	Burundi
4	BY	Belarus
5	CD	Democratic Republic of Congo
6	CF	Central African Republic (CAR)
7	CU	Cuba
8	TN	Tunisia
9	NI	Nicaragua
10	GN	Republic of Guinea
11	GW	Guinea-Bissau Republic
12	IQ	Iraq
13	IR	Iran
14	KP	Democratic People's Republic of Korea (North Korea)
15	LB	Lebanon
16	LR	Liberia
17	LY	Libya
18	ML	Mali
19	RU	The Russian Federation
20	SD	Sudan
21	SO	Somalia
22	SS	South Sudan
23	SY	Syria
24	VE	Republic of Venezuela
25	YE	Yemen
26	ZW	Zimbabwe
27	MM	Myanmar (Burma)
28	TR	Turkey
29	CN	China

INTERNAL AML PROCEDURE OF ONLINE BETTING COMPANY/ONLINE CASINO

Annex No.2

Regulation for the combating of ML/FT and Proliferation of weapons of mass
destruction

Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction

Applicable for Curaçao casinos and providers of other online games

Contents

I. Preface	3
1.1 General Statements	3
1.2 What is Money Laundering?	5
1.3 What is Financing of Terrorism?	5
1.4 What is Financing of Proliferation of weapons?	6
1.5 Targeted Financial Sanctions.....	6
II. The Risk-based Approach	7
II.1 What is the Risk-based Approach?	7
II.2 The Business and Customer Risk Assessments	8
II.2.1 Business Risk Assessment (BRA)	8
II.2.2 Customer Risk Assessment (CRA).....	9
II.2.3 Risk factors specific to the Gambling Sector	10
II.3 Technological developments risk assessment	12
III. Customer Due Diligence	13
III.1 Introduction	13
III.2 The CDD measures	14
III.2.1 Identification and verification of the player	15
III.2.2 Identification and verification of the Beneficial Owner	16
III.2.3 Obtaining information on the Purpose and Intended Nature of the Business Relationship	17
III.2.4 On-Going Monitoring	18
III.4 Enhanced Due Diligence.....	19
III.5 Simplified Due Diligence	20
III.6 Politically Exposed Persons	21
III.7 Application of CDD measures to existing customers	22
III.8 The termination of the business relationship	22
III.9 Reliance on third parties to perform customer due diligence.....	23
IV Reporting of unusual transactions.....	24
IV.1 Reporting obligations.....	24

IV.2 Prohibition of disclosure	26
IV. 3 Record Keeping	26
V Anti-Money Laundering Compliance Program	27
V.1 Introduction	27
V.2 A system of internal policies, procedures and controls.....	28
V.3 The appointment of a Compliance Officer	28
V.5 An independent audit function to test the AML program.....	31
V.6 Examination by the Gaming Control Board	31
Annex 1 Definitions	33

I. Preface

1.1 General Statements

As per February 15, 2019, the Curaçao Gaming Control Board (GCB) was officially appointed the supervisory authority for AML/CFT compliance for the whole gaming sector. This appointment is retroactive until January 1, 2016.

The NOIS, the NORUT, the Sanction National Ordinance and the Kingdom Sanction Act contain provisions for service providers to prevent those entities for being used for money laundering, the financing of terrorism and the proliferation of weapons.

The different countries act together to combat money laundering and terrorist financing in the Financial Action Taskforce on money laundering (FATF). It was established by the G-7 Summit that was held in Paris in 1989. The Dutch Kingdom is member of the FATF, Curaçao is member of Caribbean Financial Action Taskforce (CFATF). The FATF 40 Recommendations have become the world's blueprint for effective national and international control of financial crime. The FATF members incorporate the FATF Recommendations in their local laws.

The most important obligations for the gaming casino resulting from the AML/CFT laws refer to the conducting of Customer Due Diligence (CDD) and the reporting of unusual transactions. All this prevents the casino from being used by individuals for the laundering of their criminally acquired funds.

The Regulations for Combating Money Laundering, the Financing of Terrorism and Proliferation of weapons of Mass Destruction are an integral part of the land-based and the online gambling license requirements for the Curaçao jurisdiction. These Regulations are issued in implementation of:

- article 2 paragraph 8 and article 11, paragraph 3, of the National Ordinance on Identification when rendering Services (NOIS) (N.G. 2017 no. 92) and;
- article 22mm, paragraph 3, of the National Ordinance on the Reporting Unusual Transactions (NORUT) (N.G. 2017 no.99);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54).

With these Regulations the GCB offers the casinos a guideline to promote compliance with the laws and decrees with regard to money laundering, financing of terrorism and financing of proliferation and to implement sound internal policies and procedures to combat Money Laundering and the Financing of Terrorism. These include among others:

- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92);
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
- 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 decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of 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 Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).

These laws and regulations and any additional regulations issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law form the main legal basis for the Curaçao Gaming Sector to combat money laundering, the financing of terrorism and the proliferation of weapons.

As indicated, these Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction (Regulations) are applicable for Curaçao casinos (land-based and online). These regulations are effective as of May 15, 2024. There will be a transitional period of three (3) months. This implies that all land-based and online casinos are bound to comply with these Regulations as of **September 1, 2024**, at the latest.

Violation of these laws and regulations are subject to administrative and criminal sanctions.

1.2 What is Money Laundering?

All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source, can be considered money laundering (ML). It is the process of making dirty money look clean. Money Laundering consists of three phases:

- **Placement.** During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requests for pay out and inserting funds into gaming machines and immediately claiming those funds as credits;
- **Layering.** This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing moneys and hiding them from the authorities;
- **Integration.** The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples are: the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments.

Most of the people think that money laundering refers to funds acquired with drugs trafficking, but there are many predicate offences for money laundering such as human trafficking, arms trafficking, robbery, fraud, corruption, kidnapping and tax crimes.

1.3 What is Financing of Terrorism?

Financing of Terrorism (FT) is the financing of terrorist acts, of terrorists and terrorist organizations. A terrorist act is an act to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.

The most basic difference between financing of terrorism and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. Money laundering always involves the proceeds of illegal activity. There is a need for the terrorist group to disguise the link between it and its legitimate funding sources. In doing so, the terrorists use methods similar to those criminal organizations use to launder money like cash smuggling, structuring, wire transfers, purchase of monetary instruments, use of debit and credit cards. While ML is concerned with obscuring the source of funds, FT is mostly concerned with obscuring the end recipient of the funds.

1.4 What is Financing of Proliferation of weapons?

Financing of proliferation (FP) 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.

1.5 Targeted Financial Sanctions

Targeted financial sanctions require countries to freeze funds and assets and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of any designated persons or entities. All natural and legal persons in Curaçao are required to freeze without delay and without prior notice, the funds or other assets of designated persons and entities. This is to comply with United Nations Security Council resolutions and the Common Foreign and Security Policy of the European Union. Compliance with sanctions imposed by the UN Security Council is mandatory under the Charter of the United Nations. EU sanctions are binding for Curaçao on the basis of the Kingdom Sanctions Act.

At the very least, a mechanism must exist to check the sanction status of a withdrawing participant so that a sanctioned person or organization cannot remove money from an account that should be frozen. In such cases, a report must be filed with the FIU and the casino has to take the 'Process for the freezing of resources' into account.

Note: Casinos are required to check for amendments of Sanctions Decrees and Regulations on a regular basis and update their CDD- and AML/CFT-policies and - procedures accordingly to reflect such amendments.

Sanction Decrees and Regulations and amendments thereof are published on the GCB website.

II. The Risk-based Approach

II.1 What is the Risk-based Approach?

An anti-money laundering compliance program is an essential component of a casino's compliance regime. The primary goal of every good program is to protect the organization against money laundering and to ensure that the organization is in full compliance with relevant laws and regulations.

Based on the FATF Recommendations, casinos are required to apply a Risk-based Approach when designing policies, procedures and controls to combat money laundering, financing of terrorism and financing of proliferation of weapons. By adopting a Risk-based Approach, it is possible for casinos to ensure that measures to prevent or mitigate money laundering, financing of terrorism and proliferation of weapons are commensurate with the risks identified. When drawing up the anti-money laundering compliance program, a casino takes a risk-based approach. That means the higher the risk, the more measures the casino has to take to mitigate the risk. Where the risks are higher enhanced measures must be taken. Where the risks are lower they may take simplified measures, provided that this is consistent with the country's assessment of its money laundering/financing of terrorism risks.

Applying Risk-based Approach means that a casino has to:

- Assess the risks that money laundering or terrorist financing may occur within its organization beforehand;
- Design and implement appropriate policies, procedures and controls to manage and mitigate the identified and assessed risks;
- Monitor and improve the effective operation of these policies, procedures and controls;
- Document their risk assessments, including everything that has been done and the reason for this being done.

The risk assessment considers all relevant risk factors, including the player, countries or geographic areas, products and services (types of games of chance) that the casino offers and delivery channels, before determining what the level of overall risk is. Based on the risk assessment, the appropriate level and type of mitigation to be applied is determined. Casinos should also take notice of the outcomes of the National Risk Assessment (NRA) of the jurisdictions where they operate and take these outcomes into account when conducting their risk assessment.

As indicated above, casinos applying the Risk-based Approach must document their policies, procedures and controls relative to their applied Risk-based Approach. Since risks are dynamic, they must, on an on-going basis, monitor the effective operation of the policies, procedures and controls concerning their Risk-based Approach and, when needed, make the necessary amendments to these policies, procedures and controls. The risk assessment should also be made available to the GCB upon request.

II.2 The Business and Customer Risk Assessments

The bases for the risk-based approach is the risk assessment which the casino has to carry out of his own operation. This requires an understanding and assessment of risk that one's business is in general exposed to, the so-called business risk assessment.

Also each player exposes the casino to different risks. Therefore, a player-specific risk assessment must be carried out so the casino is able to identify the potential risks it faces when entering into a business relationship with, or carrying out an occasional transaction for a player, the so-called customer risk assessment. This assessment enables the operator to develop a risk profile for the customer and to categorize the ML/TF risk posed by such a player as low, medium or high.

II.2.1 Business Risk Assessment (BRA)

As indicated above, all casinos are required to carry out a business risk assessment to identify the ML/TF risks they are exposed to and ensure that the policies, controls and procedures adopted are adequate to prevent and mitigate those risks. The risk assessment should address the ways in which the casino's products and services could be used to launder money, finance terrorism and finance proliferation and the extent of the risk that this will happen. All factors that may have an impact on the risks of money laundering, financing of terrorism and financing of proliferation must be taken into account in the risk assessment, but special consideration must be given to the type of customers, products and services offered, delivery channels and geographical risk factors. Casinos have also to take into consideration and include outcomes and recommendations of the National Risk Assessment in their business risk assessment. Once the business risk has been assessed, the casino can set a risk appetite: it decides how much risk he is prepared to accept. This assists the casino in establishing and maintaining his anti-money laundering compliance program.

The effectiveness of the implementation of these measures has to be monitored and improved where necessary.

Casinos are also expected to revise their business risk assessment whenever there are changes to the environment within which they are operating and within their business activities, such as introduction of new payment methods, new markets, new games or regulatory changes. In the absence of changes, casinos have to assess their business risk at least once a year, to evaluate whether any changes thereto are necessary.

This risk assessment has to be documented and approved by the Board of directors of the casino. It should also be made available to the GCB upon request. All aspects of the Business Risk Assessment should be covered, including:

- The methodology adapted;
- The reasons for considering a risk factor as presenting a low, medium or high risk;
- The outcome of the BRA;
- Any information sources used.

In order to work risk-based, it is important that casinos continuously follow the latest reporting regarding money laundering and terrorist financing.

II.2.2 Customer Risk Assessment (CRA)

The customer specific risk assessment has to be carried out either prior to the carrying out of an occasional transaction, or during establishing a business relationship. It is possible that this initial customer specific risk assessment will have to be revised at a later stage of the business relationship and this may result in a customer's risk rating having to be adjusted.

The Customer Risk Assessment will assess the particular risks the casino will be exposed to when providing its services or products to players. The information collected to draw up the CRA will formulate the customer's risk profile. On the basis of the CRA, the proper level of CDD can then be applied as stipulated in the Customer Acceptance Policy (CAP). For this reason it is important that the casino adopts a Customer Acceptance Policy. This policy has to provide:

- a description of the type of players that are likely to pose a higher than average risk of ML/FT/FP;
- the risk indicators presenting low, medium or high risk;
- the level of Customer Due Diligence (CDD) measures, including ongoing monitoring to be applied;
- the circumstances under which service to someone is declined.

When drawing up its CAP the casino has to comply with its obligations of Politically Exposed Persons (PEP) and Sanctions Screening.

Policies, procedures and controls

Casinos must establish and maintain policies, procedures and controls to mitigate and manage effectively the risks identified in the operator's risk assessment of money laundering, terrorist financing and proliferation of weapons. The measures, policies, controls and procedures to mitigate ML/FT/FP risk are to include:

1. Customer Due Diligence (CDD);
2. Record keeping procedures;
3. Reporting procedures;
4. Risk management measures including Customer Acceptance Policies (CAP), Customer Risk Assessment (CRA) procedures, internal control, compliance management and communications of such policies, procedures and controls, employee training and employee screening policies and procedures.

It is important that these measures are clearly documented and approved by the Board of directors. The casino should monitor the implementation of those controls and enhance them if necessary. It should take enhanced measures to manage and mitigate the risks where higher risks are identified.

11.2.3 Risk factors specific to the Gambling Sector

There are four risk areas that the business risk assessment and the customer-specific risk assessment have to cover. These are:

1. Customer risk

Customer risk is the risk of ML/TF that arises from maintaining relations with a given person. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. Categories of customers whose activities may indicate a higher risk include:

- Customers who have multiple sources of income;
- Customers with irregular income streams;
- PEPs;
- High spenders (money can be derived from illegal activities);
- Disproportionate spenders (inconsistent with casino's information about customer's known source of income/assets);
- Casual customers like locals/tourists, especially when spending pattern changes;
- Improper use of third parties, criminals use third parties to gamble to break up large amount of cash, to buy chips or to cash out on behalf of others to avoid CDD measures;
- Multiple casino player rating accounts to hinder a casino to track their gambling activities;
- Unknown customers (redeeming large amounts of chips);
- Junkets (junket operators monitor player activity and issues and collect credit).

Casinos must set a value which represents the upper value of a typical player's transactions. A player having a single source of regular income will pose a lesser risk of ML/TF than a player who has multiple sources of income or irregular income streams.

2. Geographical risk

The geographical risk is the risk posed to the casino by the geographical location of the player and the source of wealth of the business relationship. The nationality, residence and place of birth of the player have to be taken into account as these might be indicative of a heightened geographical risk. Countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction and countries which are known to have terrorist organizations operating are to be considered as high risk. It is advisable to take into account a variety of sources of information produced by the FATF and non-governmental well-known bodies. Some sources to use are:

- Countries on the FATF list of High - Risk Jurisdictions subject to a Call for Action;
- Countries on the FATF list of Jurisdictions under Increased Monitoring;
- Countries on the CFATF Public Statement;
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);

- Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;
- Countries sanctioned by the OFAC;
- Countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International.

The casino must have a list of countries that are considered as high risk and those that are considered low risk.

3. *Product, service and transaction risk.*

Some products or services are inherently riskier than others and are therefore more attractive to criminals. These include products or services which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the customer to influence the outcome of a game, be it individually or in collusion with others. The use by customers and the acceptance by casinos of specific payment methods, which are considered to present a higher risk of ML/FT, should also be treated as high risk factors. These include:

- Proceeds of crime. Risk that money transferred is derived from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking and theft from employer;
- Cash. Land-based casinos (or physical establishments of online casinos) are used to exchange large amounts of illicit proceeds in small denominations for larger ones;
- Anonymous payment methods such as pre-paid cards and virtual assets;
- Use of casino accounts. This should only be done for gambling purposes and not to deposit and withdraw without gambling or minimal play;
- Types of specific games (e.g. roulette, craps → even bets);
- Peer to peer gaming;
- The use by customer of accounts held or cards issued in the name of third parties;
- The transfer of funds from one gaming account to another;
- Types of financial services (credit/marker, currency exchange, check cashing);
- Multiple casino accounts or wallets (internet operator may own and control multiple web sites);
- Changes to financial institution accounts to fund casino account;
- Identity fraud. Details of financial institution accounts stolen and used on web sites. Also stolen identities used to successfully open financial institutions accounts, and such accounts used on web sites;
- Using cash to fund a pre-paid card poses similar risks as cash;
- Games involving multiple operators (Poker on platforms shared by multiple operators);
- Electronic wallets (e- wallets). Not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits. Also, e-wallets which only accept money from financial institution accounts; the financial institution issued statements may only record the payment to the e-wallet, not the transaction to the Internet casino. This may be useful for dishonest customers who wish to disguise their gambling.

The casino must formulate a list of products or services and payment methods which are considered high risk.

4. Distribution channels risk

The channels through which a casino establishes a business relationship or through which transactions are carried out may also have an impact on the risk profile of a business relationship or a transaction:

- Channels that favor anonymity increase the risk of ML/FT if no measures are taken to address the risk;
- While situations where interaction with the customer takes place on a non-face-to-face basis no longer lead to the relationship being considered as automatically high risk, interacting in this manner is still to be considered as a high risk factor for risk assessment purposes unless the casino adopts technological measures and controls to address the heightened risk of identity fraud or impersonation present in these situations;
- Where there is the involvement of a third party in the interactions between the customer and the casino, there is also an increase of risk. This is especially the case where these third parties are not themselves subject to any form of AML/CFT obligations.

II.3 Technological developments risk assessment

A casino should maintain appropriate procedures and controls for preventing the misuse of technological developments for the purpose of money laundering or the financing of terrorism. It should identify and assess the money laundering or terrorist financing risks that may arise whenever:

- A new product is developed;
- A new business practice emerges;
- A new delivery mechanism becomes available;
- A new or developing technology is used for both new and pre-existing products.

In those cases, a risk assessment should take place prior to the launch of the new products, business practices, delivery mechanism or the use of new or developing technologies. This is done to determine whether the innovation creates a weakness that can be misused by money launderers or those seeking to finance terrorism. Such risk assessments must be documented.

Where risks are identified, measures must be taken to mitigate these risks.

III. Customer Due Diligence

III.1 Introduction

Casinos are prohibited from keeping anonymous accounts or accounts in obviously fictitious names. A casino must identify the player and ask for the player's name and other relevant information to determine the purpose and nature of the business relationship. Without sufficient knowledge, the casino may not establish or maintain a business relationship or carry out occasional transactions. A sound Customer Due Diligence program is the best way to prevent money laundering, financing of terrorism and financing of proliferation.

The customer's risk profile is essential to allow a casino to apply a certain level of Customer Due Diligence commensurate to the identified ML/TF risk. The purpose of collecting information is to provide the casino with documentation to assess the risk that may be associated with the player and to build a customer profile to assess how the player is going to act within the framework of the business relationship. Such an assessment is necessary in order to detect deviations from the expected behavior. Any unusual behavior needs to be reported to the FIU. If FIU Curaçao, after proper analysis of an unusual transaction, concludes that there is a suspicion of money laundering and/or terrorism financing, this transaction will be reported to the Public Prosecutor's Office as a suspicious transaction.

Casinos have the obligation to undertake Customer Due Diligence measures when:

- a. When players engage in financial transactions equal to or above Naf. 4,000¹;
- b. carrying out occasional transactions above the monetary equivalent of NAF. 4,000;
- c. there is a suspicion of money laundering or terrorist financing; or
- d. the casino has doubts about the veracity or adequacy of previously obtained customer identification data.

Note: a transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount in excess of the monetary equivalent of NAF. 4,000.

In case a casino carries out an occasional transaction above the monetary equivalent of NAF. 4,000, it is still obliged to apply CDD measures. Casinos are also subject to this obligation when they execute a series of linked transactions which, though individually below the applicable threshold, would cumulatively meet or exceed the NAF. 4,000 threshold. Transactions are considered as linked if for example they are carried out by the same player through the same game or in one gaming session. In this case it would be expected to apply CDD measures a and b indicated in paragraph III.2 below. In this context, the casino has to identify the player, carry out a customer risk assessment and verify the identity of the player.

Whenever an occasional transaction presents a high risk of ML/TF, the enhanced due diligence measures must be applied.

¹ The amendment of the NOIS was adopted on May 2, 2024 by Parliament. As of the date that will be mentioned in the National Gazette, CDD has to be completed when players engage in financial transactions equal to or above NAF. 4,000.

Use of physical establishments

Online casinos at times make use of physical establishments to extend their customer reach. In those situations, the customer makes use of an account held by the operator of the physical establishment to carry out transactions with the casino. In this case, the interaction between the customer and the casino is still considered to be a business relationship subject to the AML/CFT requirements of this regulation. The casino has to ensure that the physical establishment applies the casino's own AML/CFT policies and procedures.

When making use of such physical establishments, the casino also has to ensure that the operator of the establishment is of good standing. It has to identify and verify the operator of the physical establishment and monitor the activity taking place through the establishment's account so as to ensure that the operator is complying with the AML/CFT obligations. The online casino has also to regularly monitor and check whether its AML/CFT policies and procedures are properly implemented by the physical establishment. All the measures taken to guarantee compliance with the casino's measures must be documented.

III.2 The CDD measures

The CDD measures to be taken are as follows:

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

The casino, their directors, officers and employees are prohibited to disclose the fact that an UTR is being reported to the FIU. A risk exists that players could be unintentionally tipped off when the casino is seeking to perform its CDD obligations in these circumstances. Therefore, if the casino has a suspicion that transactions relate to ML or TF, he should take into account the risk of tipping-off when performing the CDD process. If the casino reasonably believes that performing the CDD process will tip-off the player, it may choose not to pursue that process, and should file an UTR to the FIU.

III.2.1 Identification and verification of the player

Identification refers to the collection of personal details of the player to establish the identity of the player. Verification on the other hand consists in confirming the personal details collected for identification purposes using reliable, independent source documents, data or information. The personal information required and extent of verification to be carried out, will vary depending on risk.

1. Identification of the player. When identifying the player, at a minimum the following information must be collected:

- i. full name;
- ii. permanent residential address;
- iii. date of birth;
- iv. place of birth;
- v. nationality; and
- vi. identity number.

However, in low risk scenarios licensees may limit identification to the three personal details set out in (i) to (iii) above. On the other hand, in high risk situations, it is possible that a licensee considers the collection of additional personal details as necessary to mitigate the higher risk of ML/FT.

2. Carry out a Customer Risk Assessment

This is done to have sufficient information available to detect unusual activity in the course of the business relationship. At this stage, a provisional risk rating will be assigned based on the initially collected information. This is revised once questions are answered or additional information received. On the basis of the CRA, the proper level of CDD can be applied as stipulated by the CAP.

3. Verification of an identity refers to actions taken to verify that a person exists and is who he claims to be. This is done by checking reliable, independent (of the person whose identity is being verified) sources.

As a rule, verification of identity has to be carried out by making reference to an unexpired government-issued document containing photographic evidence of the customer's identity (e.g. passport, identity card). Where such a document does not allow verification of the player's residential address, the casino can obtain other documents like a bank statement, utility bill, letter from a public authority or rental agreement, which should not be more than six months old to verify the residential address. The casino can also contact the player by letter, e-mail or telephone to verify the information supplied. It can also send a verification code to the e-mail address to verify that the address is current and genuine. Verification can also be done by checking social media, telephone directories, companies registries or media and news sources. Biometric checks can also be used to confirm that the individual providing the document is the one described therein.

There are also circumstances in which the casino is able to cross reference the information in his possession with geo-location information, IP address data, funding method data etc.

Verification is carried out for the casino to determine to its own satisfaction that the player is who he declared himself to be. What is important is that documents are clear, legible and of good quality. Verification of evidence of identity implies a check whether the document presented is legitimate and that it has not been stolen from the true owner. If the casino obtains foreign documentation,

extra care should be taken with regard to verifying its authenticity, particularly where the type of document is unfamiliar.

Where the casino does not have sufficient comfort that it knows its player, it is expected that it will take additional measures to do so. Some of these measures include requesting additional identification documents, asking the player to provide a photo of himself holding the ID, requiring a first payment through an account held in a reputable jurisdiction, using systems which generate codes for transmission to customers through a verified mobile phone and requiring it to be returned.

4. Sanctions screening and PEP status screening.

All players should be screened against sanctions lists of the UN and EU. If Curaçao publishes a local list with designated persons and organizations, the casino should also take that local list into account. The casino must ensure it does not do business with customers that are subject to international sanctions. Before doing business or performing an occasional transaction for the first time with a player, the casino should check published lists of known or suspected terrorists or other sanctioned persons or companies:

- U.S. Treasury's Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons List [Specially Designated Nationals And Blocked Persons List \(SDN\) Human Readable Lists | Office of Foreign Assets Control \(treasury.gov\)](#);
- EU Sanctions List <http://www.sanctionsmap.eu/#/main>.

For PEP status screening casinos can rely on internet search or consult reports and databases on corruption risk, like the Transparency International Corruption Perceptions Index or on www.knowyourcountry.com. PEPs are further addressed in paragraph III.6.

III.2.2 Identification and verification of the Beneficial Owner

Casinos in general are also required to identify and verify the identity of the beneficial owner. As a general rule, casinos should make sure that customers are registering an account to play and transact on their behalf. This can be achieved by including specific wording in the terms and conditions that a registering player must explicitly accept, together with a declaration in the form of a tick box that a player is registering to play on his/her own behalf. Casinos are not expected to merely rely on said declaration, but have to ensure that their ongoing procedures allow for the detection of possible instances where the player is actually playing on behalf of third parties.

It is acknowledged that in the majority of cases casinos will not encounter situations involving beneficial owners. However, these situations cannot be excluded completely as casinos may be maintaining business relations with one or more players funded by a syndicate. In such circumstances, where the funds being wagered are collected from multiple persons who will eventually share in any winnings, the particular transaction will not only be considered as having been undertaken by the customer but undertaken also for the benefit of those persons providing the necessary funding. These persons would be considered as beneficial owners and casinos would therefore have to identify them and verify their identity.

Where the casino's business model includes registered player accounts used by companies (corporate accounts) as a means to hedge matchbook exposure, together with business models such as the physical establishments to extend customer reach, the applicable beneficial ownership

requirement relates to the beneficial owners of the companies/operators registering those accounts. Casinos are furthermore required to distinguish between an ordinary gaming account belonging to a consumer, and such other accounts being of a different nature.

A casino must in case of business participants obtain satisfactory evidence to identify the business participants. It has to take reasonable steps to verify the identity of the beneficial owner, using information or data that was obtained from a reliable source. At the minimum identification information, verification and evidence must be gathered for all persons holding 25% or more of the shares or voting rights or a person who otherwise exercises ultimate effective control of the customer. Where no natural person is identified under the 3 items mentioned above, the natural person who holds the position of senior managing official should be identified.

III.2.3 Obtaining information on the Purpose and Intended Nature of the Business Relationship

One of the requirements of CDD is for subject persons to understand why a prospective customer is seeking to acquire a specific service or product from them. Within the context of the gambling sector, the purpose behind the opening of a gaming account is quite self-evident for which it is not required that casinos obtain any additional information from their customers.

However, this CDD measure also requires the development of a customer risk profile to have sufficient information available to allow the detection of unusual activity in the course of a business relationship. To this end, casinos have to collect sufficient information and, where it is necessary, documentation to establish a customer's source of wealth as well as the expected level of activity. Source of wealth consists of determining the activities which generate the customer's net worth and whether this justifies the projected and actual level of account activity. As to the extent of the information that casinos are to collect, it is essential that this reflects the level of ML/FT risk identified through the customer risk assessment.

Where the risk is not high, a declaration from the customer with some details (e.g. nature of employment/business, usual annual salary etc.) can be sufficient. Social media can also be used as a source of information.

However, where the risk of ML/FT is higher or casinos have doubts as to the veracity of the information collected, the information obtained would need to be substantiated by independent and reliable information and documentation. In developing a customer risk profile, casinos may also consider using statistical data to develop behavioral models against which to eventually gauge a customer's activity rather than collect source of wealth information. Where a casino opts to adopt this approach, it can use data collected from the Central Statistics Department such as average national income, average disposable income etc. These indicators should allow a casino to determine the average wagering power of players from a given jurisdiction.

The casino can also use data collected over a period of time by the casino itself, which allows the casino to create the profile of an average player. It is important to note that the reference is not to the statistical data on the individual player but to statistical data obtained from a range of players. Casinos should therefore only use this specific alternative where their customer-base is wide enough to allow the creation of an average profile. New casinos would therefore not be expected to use this method unless they are able to obtain gaming data from another casino offering the same games within the same markets and having a similar business model to the one being adopted by the new casino.

It is important to note that the use of statistical data is incompatible with high risk situations as the transactional pattern will fall outside the average behavioral model. In such circumstances, casinos would have to collect source of wealth information as set out above.

In developing a customer business and risk profile, casinos form the basis for the scrutiny of activity required to meet part of their on-going monitoring obligation.

III.2.4 On-Going Monitoring

The casino must conduct ongoing due diligence on the business relationship and scrutinize the transactions undertaken throughout the course of that relationship to ensure that they are consistent with the casino's knowledge of the customer, the customer's business and risk profile.

Ongoing monitoring of identity

In conducting ongoing due diligence on the business relationship the casino should hold accurate and up to date identification data of its customers. Since identity may change due to circumstances, the casino should be able to show that if identification information changes, it will be detected and re-evidenced. This means that the casino should consider to obtain evidence of identity periodically to detect any changes, refresh the data on key events (i.e. change of payment instrument) or should consider tracking expiry dates on evidence of identity and refreshing it as it expires. Casinos should determine on a risk-sensitive basis whether changes are substantial as to require re-assessment of customer risk of the business relationship.

Ongoing monitoring of transactions

Transaction monitoring is executed to prevent involvement of the casino with ML/TF and to safeguard the reputation of the casino. While in conducting ongoing scrutiny of transactions a casino notices that a customer's transactions are not consistent with what it knows or expects from the customer, the casino has to question this unusual activity and, where necessary, establish the source of the funds used for that transaction. Source of funds refers to how the funds for a particular transaction were obtained by the player. The reason for inconsistency may lie in inconsistency, amongst others, with the source of funds or average profile or account activity noted to date). The casino has to understand what the reason for this deviation is and obtain sufficient information and documentation with regard to the transaction. It is also one of the situations in which the risk profile of the customer may have to be revised.

After receiving this information the casino has to decide whether the transaction is an unusual transaction and need to be reported to the FIU.

As with anything else, the level of on-going monitoring will depend on the risk profile of the customer, but even in low risk situations there must be a degree of oversight taking place to ensure that the business relationship still has to be considered as a low risk one.

III.3 Timing of CDD Measures

A casino provides services to a customer allowing for the wagering of a stake with monetary value in a game of chance. They do business with customers that are individuals and who act in their own name and on their own behalf. In doing so they open an account for their customers or the player becomes a member of the player club. This is considered to be indicative of a relationship that is expected to have an element of duration and is therefore considered a business relationship between the casino and its customer. For casinos, verification of identity has to be conducted when engaging in financial transactions equal to or in excess of Naf. 4,000. This implies that all CDD measures must have been conducted at the time the threshold is reached. However, casinos are required to apply a minimum level of CDD measures prior to reaching the threshold. Thus, simultaneously with the opening of an account, casinos are to identify the customer by collecting the minimum personal details, being: name and surname, permanent residential address and date of birth (set as the minimum applicable in case of low risk business relationships) and conduct the sanctions screening. The threshold is to be calculated on a daily basis taking into account all deposits and withdrawals made by the player since the establishment of the business relationship, including any peer-to-peer transfers. Once the threshold is reached, casinos have to conduct PEP status screening and carry out a customer risk assessment and meet their remaining CDD obligations as indicated in paragraph III.2 above.

Carrying out CDD as early as possible can limit situations in which a casino receives contaminated funds. For land-based casinos it is therefore advisable to carry out CDD when establishing a business relation and not to wait until the threshold is reached.

In carrying out the CDD measures, customers may be allowed to continue using their gaming account while the casino obtains any necessary information from the customer concerned. However, if the Naf. 4,000 threshold is reached, the player cannot deposit funds into the account or withdraw funds from the account.

Besides that, if the requested information and documentation is not received within 30 days from the moment the Naf. 4,000 threshold was met in order for the casino to complete CDD, the casino has to terminate the relationship with the player and report the transaction to the FIU.

III.4 Enhanced Due Diligence

A risk-based approach should be taken, so more thorough checks should be undertaken for higher risk customers. The Enhanced Due Diligence (EDD) measures should be consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual. Enhanced Due Diligence **has to** be conducted where the risks of money laundering or terrorist financing are higher. This concerns for example:

- Residents of higher risk geographic areas;
- Political Exposed Persons (PEP's);
- Products or transactions that might favor anonymity;
- New products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

The applied measures must be consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of enhanced due diligence measures include:

- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the source of funds or source of wealth of the player. Examples of source of funds include personal savings, employment, pension releases, share sales and dividends, property sales, gambling winnings, inheritances and gifts and compensation from legal rulings;
- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship;
- Conducting enhanced monitoring of the business relationship;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

In situations presenting a higher risk of ML/TF, source of funds information has to be requested from time to time even though there may not be any change in pattern or activity conducted by the customer.

III.5 Simplified Due Diligence

Where the risks of money laundering or terrorist financing are lower, casinos **are allowed** to conduct simplified CDD measures, which should take into account the nature of the lower risk. Examples of possible measures:

- Not collecting specific information. If the risk assessment undertaken indicates a low risk of money laundering or terrorist financing then it is only necessary for the casino to obtain the player's identity. In this case casinos may limit identification to the first three personal details in paragraph III.2.1.
- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;
- The extent of verification may also vary depending on the risk posed by the particular business relationship. In a low risk situation, the casino can also use alternative reputable information sources, even where these do not contain photographic evidence of the player's identity (e.g. birth certificates, bank statements etc.);
- The extent of personal details verified can also vary. In low risk situations, the casino has to verify the basic identification details, while the verification of any other personal details is upon the casino, as long as it has sufficient comfort that it knows who its customer is;
- Reducing the frequency of customer identification updates;

- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

III.6 Politically Exposed Persons

A casino is required, in relation to foreign politically exposed persons (PEPs), (whether as customer or beneficial owner) in addition to performing normal customer due diligence measures, to:

- have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;
- obtain senior management approval to service the PEP (for establishing the business relationship for new customers, continuing the business relationship for existing customers or for conducting the occasional transaction). Senior management are the persons who determine the day-to-day operations or those directly below the level of those determining the day-to-day operations. The approval can also be from the manager of the Compliance department;
- take reasonable measures to establish the source of wealth and the source of funds. The investigation must then determine whether the player's spending pattern matches his legal source of funds. The casino requests a statement from the player about the source of funds and verifies them by consulting independent and reliable sources. Depending on the risk in specific cases, this can in the first place be public sources. When public sources cannot, or can insufficiently verify the received information, the casino can request the customer to provide documents; and
- conduct enhanced ongoing monitoring of the business relationship.

A casino is required to take reasonable measures to determine whether a customer is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. In cases of a higher risk business relationship with such persons, casinos are required to apply the measures referred to in items b, c and d.

Although stricter customer due diligence is required for each PEP, this customer due diligence does not be the same for every PEP. The measures are tailored to the risk of the PEP, where the following is taken into consideration:

- the type of public function of the PEP;
- the country from which the PEP originates;
- the transactions that the PEP carries out.

This means that the measures taken can be tailored to the risks in a specific case.

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

Screening for PEP status has to be carried out before establishing the business relationship or conducting the occasional transaction. In addition, the casino must regularly screen for PEP status during the business relationship. Should a player who had not been identified as a PEP at on-boarding stage result to have become one, the casino is required to implement the measures

described above within the thirty day window. Failing with these, will result in the casino to terminate the relationship with this customer.

III.7 Application of CDD measures to existing customers

Casinos should also apply the CDD measures to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times. Casinos have to consider whether any procedures they have been applying are sufficient to meet their CDD obligations as indicated in this chapter. If this is the case, they can continue applying these and pay special attention to their on-going monitoring obligations as set out in this chapter.

If the casino had no procedures in place to meet the CDD requirements, it has to apply these on a risk sensitive basis and must conduct customer due diligence on such existing relationships on appropriate times².

III.8 The termination of the business relationship

In case the obligations arising from the customer due diligence (paragraph III.2) cannot be met, the casino cannot establish the business relation or perform the transaction or he is obliged to terminate the business relationship with the customer. The casino must also keep a record of all the attempts made to get the necessary information and documentation. To this end, a casino may decide to either close the account or to keep it blocked and suspended in its entirety.

In the event that the customer makes the requested information and/or documentation available to the casino following the closure or the suspension and blocking of the gaming account, the casino has to consider whether the delay in providing the requested CDD documentation and/or information affects the risk of ML/FT associated with the given business relationship.

The casino is to consider whether there are any grounds giving rise to suspicion of ML/TF/FP. The reluctance of the customer to provide CDD on its own should not be automatically equated to a suspicion of ML/TF/FP. The casino should consider all factors and information it has at his disposal to decide whether there are grounds to suspect ML/FT/FP. If, however the presumption of ML/FT/FP exist the casino should submit an unusual transaction report to the FIU with regard to this player.

Where there is no reason for the retention of funds, the funds are to be remitted back to the player. This has to be done through the same channels used to receive the funds.

² After amendment of the NOIS this has to be done when the player has met the Naf. 4,000 threshold.

III.9 Reliance on third parties to perform customer due diligence.

Gambling companies may rely on third parties when performing elements a-c of the CDD measures in paragraph II.2 above, provided that the criteria set out below are met. The third party should be subject to CDD and record-keeping requirements. The third party will have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying institution. Where such reliance is permitted, the ultimate responsibilities for CDD measures remains with the casino relying on the third party. The criteria to be met are as follows:

1. A casino has to obtain the information concerning elements a-c of the CDD measures immediately from the third party it is relying upon;
2. The casino should have an agreement with the third party being relied upon that copies identification data or other relevant documentation relating to CDD requirements will be made available upon request and this arrangement must be tested from time to time to ensure that it actually functions as set out in the agreement. The casino however, remains responsible for the carrying out of a customer-based risk assessment, determining whether the customer is a PEP and conducting on-going monitoring;
3. The casino should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and recordkeeping requirements as described in this regulation. The third party will have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying institution, and would apply its own procedures to perform CDD measures;
4. When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

This is different to the outsourcing/agency scenario, in which the outsourced entity applies the CDD measures on behalf of the delegating casino, in accordance with its procedures, and is subject to the delegating casino's control of the effective implementation of those procedures by the outsourced company. It is important that the casino is aware that it will remain responsible at all times for compliance with said regulations. For this reason there should be periodical assessments of how the service provider is fulfilling its obligations under the outsourcing arrangement both quantitatively as well as qualitatively. However, the decision whether to on-board a customer or to continue a business relationship on the basis of risk cannot be outsourced.

Any activity performed by an agent or group company is to be considered as an activity performed by the casino. As such, any customer on-boarded by the agent or group company has to undergo the same checks and controls as customers on-boarded by the casino itself. It is therefore up to the casino to ensure that its AML/CFT controls, policies, measures and procedures are applied by the agent or group company.

IV Reporting of unusual transactions

IV.1 Reporting obligations

Gambling companies are not only required to adhere to the stipulations of the National Ordinance for Identification of Services, but are also required to detect and report either intended or completed unusual transactions. It is important for every casino to have adequate procedures in place that cover the following:

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

Recognition of unusual transactions

An unusual transaction is a transaction inconsistent with the player's profile. Therefore, the first key to recognizing that a transaction or series of transactions is unusual is to know enough about the player. The purpose of collecting information is to provide the casino with documentation to assess the risk that may be associated with the player and to build a customer profile to assess how the player is going to act within the framework of the business relationship.

Based on the NORUT legislation, objective and subjective indicators have been established by means of which casinos must assess whether a customer's transaction qualifies as an unusual transaction. Management must provide its staff with specific guidance and training in recognizing and adequately documenting unusual transactions. All these unusual transactions must be reported to the compliance officer in the format approved by management. All additional documents available, such as copies of identification documents, cash out slips, and other records must be also submitted as supplements. The compliance officer must keep an adequate filing system of these records. If internally reported transactions are not reported to the FIU by the casino, the reason shall be adequately documented and signed off by the compliance officer and/or management.

In order to implement FATF recommendation 11, gambling companies must pay special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

The following transactions or intended transactions are deemed unusual³:

- a. Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- b. Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c. Transactions in the amount of NAf. 5,000 or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means. This includes but is not limited to:

• ³ Ministerial Decree with general operation of December 1, 2015, laying down the indicators, as mentioned in article 10 of the NORUT (Decree Indicators Unusual Transactions) (N.G. 2015 no. 73).

1. A cashless transaction in the amount of NAf. 5,000 or more.
A cashless transaction is a transfer from a bank account of the casino to a local or international bank account, at the request of the client.
2. Accepting or releasing a deposit in the amount of NAf. 5,000 or more at the request of the client;
3. Sale to a customer of chips in the amount of NAf. 5,000 or more. "Chips" include but is not limited to tokens and credits.
4. A cash out in the amount of NAf. 5,000 or more;

Note: A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of NAf. 5,000.

d. Presumed money laundering transactions or terrorist financing: Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Reporting of unusual transactions

By virtue of article 11 of the NORUT, the casino must report unusual transaction or any intended unusual transaction to the FIU without delay. In order to do this, they should have clear procedures for internal and external reporting of unusual transactions in place. These should be communicated to their personnel.

All unusual individual transactions or series of transactions, as mentioned in the Regulation Indicators Unusual Transactions, must be reported internally, without any delay. Also supporting documents must be submitted as part of the reporting.

The documentation of unusual transactions

Each casino has to register with the FIU and to get access to the goAML reporting portal after validation by the FIU.

The compliance officer must prepare a report of all unusual transactions for external reporting to the FIU according to the reporting regulations of the FIU. The casino shall report to the FIU the details of the transactions by means of the goAML reporting portal. The reports and the submission of the thereto related information (all supporting documents) should be done in English.

The casino and its directors, officers and employees are protected by law from criminal and civil liability for breach of any restriction on disclosure of information when reporting to the FIU.

IV.2 Prohibition of disclosure

A casino and its senior management and employees shall not disclose any details or information in connection with a report filed to the FIU or a request for information made by the FIU. They are not permitted to disclose information to the customer nor to third parties. The reason for this is not to jeopardize an analysis or investigation into Money laundering or Terrorist financing. This is also the reason why caution is advised when a casino takes action to terminate a relationship or otherwise block additional transactions following reporting to the FIU. Drastic action should only be taken when there is no other way out, since any unjustified action may alert the player. In such circumstances, it would be more advisable to increase on-going monitoring and submit additional reports to the FIU on any other suspected instances of ML/TF.

IV. 3 Record Keeping

Casinos shall maintain, for at least five years, all necessary records on transactions (both domestic and international), to enable them to comply with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide , if necessary, evidence for prosecution of criminal activity.

All records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence must be kept for at least five years after the business relationship is ended, or after the date of the occasional transaction.

The CDD information and the transaction records should be available to domestic competent authorities based upon appropriate legal authority.

V Anti-Money Laundering Compliance Program

V.1 Introduction

An anti-money laundering program is an essential component of a casino's compliance regime. The primary goal of every good program is to protect the organization against money laundering and to ensure that the organization is in full compliance with relevant laws and regulations. For that reason, designing, structuring and implementing these programs should be the top priorities of any institution. An AML program should be risk-based, and should be designed to mitigate the money laundering and terrorist financing risks the organization may encounter. The AML program should establish minimum standards for the organization that are reasonably designed to comply with applicable laws and regulations. The organization-wide program should be supplemented by the policies and procedures of the institution.

Before designing an AML program, it is imperative to understand what is required of an institution, its employees and customers by the laws and regulations of Curaçao.

The basic elements a casino must address in an anti-money laundering compliance program are:

1. A system of internal policies, procedures and controls;
2. A designated compliance officer with day-to-day oversight over the AML program;
3. An employee screening program and ongoing employee training program; and
4. An independent audit function to test the AML program.

The anti-money laundering program also ensures that the obligations regarding customer due diligence, reporting unusual transactions, retention periods, data protection and training are met. The casino tests the anti-money laundering program systematically and adapts the program to the current risks that arise within the company's own organization. The AML program has the approval of senior management.

Casinos must ensure that their foreign branches and subsidiaries, if any, implement AML/CFT/CFP measures consistent with the requirements of Curaçao.

V.2 A system of internal policies, procedures and controls

All casinos must have policies and procedures, including a policy statement in place that clearly expresses the casino senior management's commitment to combat the abuse of its facilities, products and services for the purpose of money laundering, terrorist financing and the proliferation of weapons of mass destruction purposes. The policies shall state the casino's intention to comply with current anti-money laundering, combating the financing of terrorism and financing of proliferation legislation as well as regulations, in particular the laws and regulations regarding customer due diligence, the reporting of unusual transactions and keeping adequate records of clients and transactions (NOIS, NORUT, Sanctions National Ordinance, Kingdom Sanction Act. They should set the tone for the organization.

The standard AML operating procedures are more detailed than the policies. They translate policy into an acceptable and workable practice. Casinos shall also have a process in place to stay on top of regulatory changes, which should keep the program current.

While policies and procedures provide important guidance, the AML program also relies on a variety of internal controls. These internal controls should enable the compliance officer to recognize deviations from standard procedures and protocols.

The anti-money laundering policies and procedures should be in writing and shall be approved by senior management or the board of directors. The casino's policies and procedures shall be communicated to its employees.

V.3 The appointment of a Compliance Officer

The casino shall formally designate a senior officer at management level and independent from the games operations, responsible for the detection and deterrence of money laundering and terrorist financing. The AML/CFT compliance officer must have timely access to customer identification data and other CDD information, transaction records, and other relevant information. The compliance officer must be able to act independently. 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.

The above-mentioned responsibilities shall be included in the job description of the compliance officer. The job description shall be signed off and dated by the officer, indicating his/her acceptance of the entrusted responsibilities.

V.4 Employee screening program and ongoing employee training program

Casinos shall ensure that their business is conducted at a high ethical standard and that the laws and regulations pertaining to financial transactions are followed. Each casino shall establish and adhere to proper policies and procedures in screening their employees for criminal records.

Casinos shall develop training programs and provide training to all personnel who handle transactions that may be qualified as unusual based on the indicators outlined in the Ministerial Decree regarding the Indicators for Unusual Transactions (N.G. 2015 no. 73).

Training includes setting out rules of conduct governing employee's behavior and their ongoing education to create awareness of the casino's policies against money laundering and terrorist financing. Most areas of the institution should receive training, and the target audience should include most employees. But each segment should be trained on topics and issues that are relevant to them. Training must at least address the following topics:

a) New employees

A general training of the nature and process of money laundering and terrorist financing, and the need to report any unusual transactions to the appropriate designated officer must be provided to all new employees who will handle customers or their transactions, irrespective of their level of seniority. They shall be made aware of the existing internal policies, procedures and regulations concerning money laundering, terrorist financing, proliferation of weapons and the reporting requirements. They must also be trained on the money laundering methods and trends in the gambling sector. They must receive an explanation on customer due diligence and objective and subjective indicators for reporting unusual transactions.

b) Dealers, cashiers and slot department personnel

This is your front line of defense against money laundering. They will need a general course to address the importance of AML and to provide some basics. They need some additional training on how money launderers might use gambling companies to launder money. They also need some training on the organization's procedures in order for them to know what they must do if they recognize potential money laundering. Personnel involved with account opening must also understand the need to verify the identity of the customer.

c) Audit staff

Those charged with overseeing, monitoring and testing money laundering controls should also be trained about changes in regulation, money laundering methods and enforcement, and their impact on the organization.

d) AML Compliance staff

These are the people who run the AML program. They will need specialized training to be able to stay on top of new trends or changes that impact the organization and the way it manages risk. This will require attending conferences or AML-specific presentations to go into greater detail.

e) Supervisors and Managers

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

f) Senior management and board of directors

Money laundering issues and dangers should be regularly and thoroughly communicated to the board. This to keep board members aware of the reputational risk that money laundering poses to the institution.

Refreshment training must be arranged at regular intervals to ensure that staff members are kept informed of current and new developments regarding money laundering and terrorist financing techniques, methods and trends. To demonstrate compliance with aforementioned staff training guidelines, the casino shall maintain records that include:

- 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.

V.5 An independent audit function to test the AML program

The AML compliance program must be monitored and evaluated at least annually by an adequately resourced internal audit department or an outside independent party. The audit must be independent, thus performed by people not involved with the organization's AML compliance staff. Those performing the audit must be sufficiently qualified to ensure that their findings and conclusions are reliable. These tests must include at least:

- An evaluation of the institution's anti- money laundering, counter terrorist financing and counter financing of proliferation manuals;
- Customer's file review;
- Compliance management;
- Performance of transaction testing;
- Assessment of training adequacy;
- Assessment of compliance with applicable laws and regulations;
- Evaluation of the system's ability to identify unusual activity;
- Interviews with employees who handle transactions and with their supervisors;
- A sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- An assessment of the adequacy of the record retention system.

The audit team should also consider whether the board was responsive to earlier audit findings. The scope of the testing and the testing results must be documented, with any deficiencies reported to senior management and/or the Board of Supervisory Directors, and to the designated officers with a request to take prompt corrective actions by a certain deadline. These corrective actions could also include enhancement of controls and procedures.

V.6 Examination by the Gaming Control Board

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

- a. Its written and approved AML Compliance Program on money laundering, terrorist financing and financing of proliferation;
- b. Records of its Business Risk assessment;
- c. The name of each Compliance Officer responsible for the casino's overall money laundering and terrorist financing policies and procedures and his/her designated job description;
- d. Records of reported unusual transactions;
- e. Records of unusual transactions which required closer investigations;
- f. Records of frozen accounts;
- g. Schedule of the training provided to the casino's personnel regarding money laundering, terrorist financing and proliferation of weapons;

- h. The assessment report on the casino's policies and procedures on money laundering, terrorist financing and financing of proliferation by the internal audit department or an external auditor;
- i. The customer's files including customer risk assessment, CDD, customer acceptance and transaction information.

Annex 1 Definitions

In these regulations the following definitions are used:

Casino

In these Regulations includes both land-based and online casinos.

CFATF

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. 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. 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

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. In casinos these 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.

FIU

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

Kingdom Sanctions Act

The National Ordinance also known as the “Rijkssanctiewet”, published under N.G. 2016 no. 54.

NOIS

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

NORUT

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

Other online games

Includes sports betting, esports betting, fantasy sports, lottery and bingo, skill-based games and virtual sports.

Politically Exposed Persons (PEPs)

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

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

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.

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.