CGA
Curaçao Gaming Authority

REGULATIONS FOR THE COMBATING OF MONEY LAUNDERING, THE FINANCING OF TERRORISM AND PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

Applicable to Curaçao casinos and providers of other online games

November 2026

Contents

I. Preface 1

1.1 General Statements 4

I.2 What is Money Laundering? 6

I.3 What is Financing of Terrorism? 6

I.4 What is Financing of Proliferation of weapons? 7

I.5 Targeted Financial Sanctions 7

II. The Risk-based Approach 8

II.1 What is the Risk-based Approach? 8

II.2 The Business and Customer Risk Assessments 9

II.2.1 Business Risk Assessment (BRA) 9

II.2.2 Customer Risk Assessment (CRA) 10

II.2.3 Risk factors specific to the Gambling Sector 11

II.3 Technological developments risk assessment 13

III. Customer Due Diligence 14

III.1 Introduction 14

III.2 The CDD measures 15

III.2.1 Identification and verification of the player 16

III.2.2 Identification and verification of the Beneficial Owner 17

III.2.3 Obtaining information on the Purpose and Intended Nature of the Business Relationship 18

III.2.4 On-Going Monitoring 19

III.3 Timing of CDD Measures 20

III.4 Enhanced Due Diligence 22

III.5 Simplified Due Diligence 23

III.6 Politically Exposed Persons 23

III.7 Application of CDD measures to existing customers 24

III.8 The termination of the business relationship 25

III.9 Reliance on third parties to perform customer due diligence. 25

IV Reporting of unusual transactions 27

IV.1 Reporting obligations 27

IV.2 Prohibition of disclosure 29

IV. 3 Record Keeping 29

V Anti-Money Laundering Compliance Program 30

V.1 Introduction 30
V.2 A system of internal policies, procedures and controls 31
V.3 The appointment of a Compliance Officer 31
V.4 Employee screening program and ongoing employee training program 32
V.5 An independent audit function to test the AML program 34
V.6 Examination by the Gaming Control Board 34
Annex 1 Definitions 36

I. Preface

1.1 General Statements

As per February 15, 2019, the Curaçao Gaming Control Board (CGA) 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.

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 (ML/FT/FP) 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 CGA 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);
- Omnibus Sanctions Decree (N.G. 2025 no. 52 as amended;
- 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 to Curaçao casinos (land-based and online) offering games of chance and other online games. These regulations are effective as of November 1, 2026. 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 **February 1, 2027**, at the latest.

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

I.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 requesting 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.

I.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.

I.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. Persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant sanctions programs.

I.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'[1] 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 CGA website.

[1] Refers to the Process for the freezing of resources (Proces bevriezing van middelen) for the implementation of sanctions imposed by international organizations published in the National Gazette on September 16, 2016.

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 casinos are encouraged to 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, terrorist financing or proliferation financing may occur within its organization beforehand;
- Design and implement appropriate policies, procedures and controls, which are approved by senior management, to enable them to manage and mitigate the risks that have been identified;
- Monitor and improve the effective implementation of these policies, procedures and controls;

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, casinos 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.

II.2 The Business and Customer Risk Assessments

The basis 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 Money laundering, Terrorist Financing and Proliferation Financing 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 it is prepared to accept. This assists the casino in establishing and maintaining its anti-money laundering compliance program.

The Business Risk assessment has to be documented and casinos are also expected to keep these assessments up to date. 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, the BRA shall be reviewed. 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.
Casinos shall have appropriate mechanisms in place to provide risk assessment information to the CGA and other competent authorities 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 developments 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 with regard to 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.

II.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 and break up large amounts of cash, to buy chips or to cash out on behalf of others to avoid CDD measures;
- Customers using 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 well-known 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 having 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 of 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 after 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 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 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. players engage in financial transactions equal to or above XCG 4,000;
b. carrying out occasional transactions[2] above the monetary equivalent of XCG 4,000[3];
c. there is a suspicion of money laundering or terrorist financing; or
d. they have doubts about the veracity or adequacy of previously obtained customer identification data.

In case a casino carries out an occasional transaction above the monetary equivalent of XCG 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 XCG 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.

[2] An occasional transaction refers to a transaction with a one-off customer, that at that point, is not expected to return. This applies typically to land-based casinos, where no opening of an account is required to play.
[3] 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 XCG 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 AML/CFT/CFP policies and procedures 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, its source of funds.

The casino, its 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, it 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 a report 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 of 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[4].

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[5], 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.

[4] If the player is required to open an account for playing demo games and that account can be used for paid games as well, the casino needs to collect personal information of the player at this stage.
[5] For phone bills, only fixed line telephone bills are accepted as proof of address.

There are also circumstances in which the casino is able to cross reference the information in its possession with geo-location information, IP address data, funding method data etc.
Verification is carried out by 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 when the type of document is unfamiliar.

When the casino does not have sufficient comfort that it knows its player, it is expected to 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, EU and the Netherlands. 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 through[6]:

- United Nations Security Council Consolidated List https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list
- EU Consolidated Sanctions List **http://www.sanctionsmap.eu/#/main;**
- Nationale sanctielijst terrorisme https://www.rijksoverheid.nl/documenten/2015/08/27/nationale-terrorismelijst

For PEP status screening casinos can rely on internet search or consult reports and databases on corruption risk, like www.knowyourcountry.com. For local PEPs, the PEP Caribbean list can be consulted. 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.

[6] See also the CGA Guidance on Compliance with Sanctions Regulations (2026).

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 identities.

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.

In case of business participants a casino must obtain satisfactory evidence to identify these 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 and 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 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 of 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 business model similar 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 in which the transactional pattern will deviate from 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 demonstrate 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 when expiring. 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 performing 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 these transactions. Source of funds refers to how the funds for a particular transaction were obtained by the player. The reason for above inconsistency

may be deviation, amongst others, from 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. This 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. It does business with customers that are individuals and act in their own name and on their own behalf. In doing so it opens an account for its customers or latter 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 therefore is 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 XCG 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 requirements in case of low risk business relationships) and conduct the PEP status screening and 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 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 to have the verification completed.

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 XCG 4,000 threshold is reached because of a deposit of the player, he cannot further deposit funds into the account or withdraw funds from the account. He still will be able to play, using the funds already in his account. However, if the XCG 4,000 threshold is reached because the customer wants to withdraw his money, a complete freezing of the account should occur. In this case it will not be possible for the customer to continue playing.
Besides that, if the requested information and documentation is not received within 30 days from the moment the XCG 4,000 threshold was reached, the casino has to terminate the relationship with the player and report the transaction to the FIU if a presumption of money laundering or terrorist financing exists. If no presumption of money laundering exists, the funds should be transferred to the same bank account or wallet it was deposited from. If presumption of money laundering or terrorist financing exists, internal procedures should indicate whether the funds are

blocked or not. Consideration should be given to the fact that by blocking the account, the customer may be tipped off.

III.4 Enhanced Due Diligence

A risk-based approach should be applied, implying more thorough checks should be performed for higher risk customers. The Enhanced Due Diligence (EDD) measures should be consistent with the risks identified. In particular, a casino should increase the degree and nature of monitoring of the business relationship, in order to determine whether 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 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 the nature of the lower risk into account. 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;
- Adapting verification to perceived risk. 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.);
- Limiting the extent of personal details to be verified. In low risk situations, the casino has to verify the basic identification details , while the verification of any other personal details is to the discretion of 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

In relation to foreign politically exposed persons (PEPs), whether being customers or beneficial owners, in addition to performing normal customer due diligence measures, a casino is required to:

a. have appropriate risk-management systems in place to determine whether the customer or the beneficial owner is a politically exposed person;

b. 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 obtained from the manager of the Compliance department;

c. 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 that by consulting independent and reliable sources. Depending on the risk in specific cases, these 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 additional documents; and

d. 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 have to be the same for every PEP. The measures are tailored to the risk of the PEP, with the following being 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 identified in a specific case.
The requirements for all types of PEPs should also apply to family members or close associates of such PEPs.

Screening for PEP status has to be carried out at on-boarding as indicated in paragraph III.2.1. 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 become one, the casino is required to implement the measures described above within the thirty-day window of observing that the person is a PEP. Failing with these, shall result in the casino terminating 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 a 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 at appropriate times[7].

[7] The amendment of the NOIS was adopted on May 2, 2024 by Parliament. As of May 15, 2024 CDD has to be completed when players engage in financial transactions equal to or above XCG 4,000.

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 and 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 exists 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.

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

Casinos 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 of the casino. 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 (casino). Where such reliance is permitted, the ultimate responsibilities for CDD measures remain with the casino relying on the third party. The criteria to be met are as follows:

1. The 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, casinos should have regard to information available on the level of country risk.

For casinos that rely on a third party that is part of the same financial group, the group CDD and record-keeping requirements that the foreign branches and subsidiaries apply should be consistent with Curaçao laws and regulations. The group's AML/CFT policies should adequately mitigate any potential risk from a higher-risk country. The implementation of those CDD and record-keeping requirements and AML/CFT programs is supervised at a group level and any higher country risk is adequately mitigated by the group's AML/CFT policies.

The above-mentioned reliance on third parties 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 and 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 the responsibility of 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

Casinos 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 that every casino has 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 player 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 reasons therefore shall be adequately documented and signed off by the compliance officer and/or management.

In order to implement FATF recommendation 11, casinos 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 unusual[8]:

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 XCG 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:

   1. A cashless transaction in the amount of XCG 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;

[8] 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).

2. Accepting or releasing a deposit in the amount of XCG 5,000 or more at the request of the client;
3. Sale to a customer of chips in the amount of XCG 5,000 or more. "Chips" include but is not limited to tokens and credits;
4. A cash out in the amount of XCG 5,000 or more[9];

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 XCG 5,000 or more and is considered per gaming day.

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, it should have clear procedures for internal and external reporting of unusual transactions in place. These should be communicated to its 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 obtain access to the goAML reporting portal after validation by the FIU. The FIU allows bulk reporting, therefore the casino account manager at the FIU should be contacted in order for the FIU to determine if the operator qualifies for this service.

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 these 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.

[9] The indicated examples are not limited, also credit card transactions and e-wallet transactions are to be reported 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 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, to enable the casino to manage and mitigate the risks that have been identified. The casino's policies and procedures shall be communicated to its employees.
Since risks are dynamic, the casino must, on an on-going basis, monitor the effective operation of the policies, procedures and controls and make the necessary amendments to these policies, procedures and controls.

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 design an internal procedure about when reporting of unusual transactions will lead to blocking/ freezing of user accounts, taking into account the risk of tipping off the player.

- 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 employees' 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 the 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 casinos 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[10] 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 CGA in preparation of or during an examination and upon CGA 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;

[10] The auditor must have at least two years of experience in AML/CFT compliance along with a bachelor's degree and a relevant AML certification. Recognized certifications include the CAMS or CAMS-Audit certification from the ACAMS or AMLFC certification from the AML Foundation & Compliance Institute.

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 land-based 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. In online casinos, financial transactions are deposits and withdrawals (bonusses are not included). Amounts wagered and winnings are considered as gambling transactions. Gambling transactions are not considered as financial transactions.

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.