



CAECUS N.V.

163779

Chuchubiweg 17, Willemstad, Curaçao

AML/CTF/CPF POLICY

Version 1 / 2024

APPROVED BY THE BOARD OF DIRECTORS

A handwritten signature in blue ink, consisting of a large, stylized letter 'A' followed by a series of loops and a final stroke that extends to the right.

DATE 11/11/2024

A small, handwritten signature in blue ink, consisting of a single, stylized letter 'f'.

TABLE OF CONTENTS

1. Definitions	4
2. Statement of the Policy	8
3. Overview of the Online Gaming Environment	9
4. Understanding Money Laundering & Terrorism Financing	9
5. Assessment of Risks Related to Money Laundering, Terrorist Financing, and Proliferation Financing	11
5.1. Fundamental Elements of the Risk-Based Strategy	12
5.2. Adherence to Curaçao's Recent Legislation	13
5.3. Unique Risks Associated with the Gambling Sector	13
6. Customer Due Diligence	14
6.1. Conditions for Implementing CDD Measure	14
6.2. Components of the CDD Process	15
6.3. Player Identity Establishment	15
6.4. Understanding Player Relationships	16
6.5. Continuous Surveillance	16
6.6. Enhanced Investigation for High-Risk Cases	16
6.7. Simplified Verification for Low-Risk Cases	16
6.8. Special Considerations for Politically Exposed Persons (PEPs)	17
6.9. Relationship Termination Protocol	17
7. Sanctions Compliance	17
7.1. Monitoring and Reporting Procedures	17
7.2. Client Interaction and Transaction Verification	17
7.3. Continuous Review of Compliance Procedures	18
7.4. Due Diligence and Evasion Prevention	18
7.5. Staff Training and Auditing	18
8. Management Responsibilities	18
8.1. Policy Review and Risk Assessment	18
8.2. Employee Training Programs	19

8.3. Internal Control Framework	19
9. Compliance Officer	19
9.1. Designation and Authority	19
9.2. Key Functions of the Compliance Officer	19
9.3. Core Responsibilities	20
9.4. Conclusion	20
10. Detection and Reporting of Suspicious Activity	20
10.1. Characteristics of Unusual Transactions	21
10.2. Assessment and Reporting Procedures	21
10.3. Confidentiality of Reporting Process	21
11. Audit Procedures	21
11.1. Objectives of the Audit	21
11.2. Auditor Appointment	22
11.3. Adherence to Standards	22
11.4. Audit Reporting	22
11.5. Oversight by the Gaming Control Board	22
11.6. Consequences of Non-Compliance	22
12. Record Keeping	23
13. Training	23
13.1. Role-Specific Training Requirements	23
13.2. Training Structure	24
13.3. Training Curriculum Content	24
13.4. Delivery Methods	24
13.5. Qualified Trainers	24

1. Definitions

Suspicious Activity Report/Suspicious Transaction Report – **SAR/STR**

Counter Proliferation Financing – **CPF**

A senior management member who maintains independence from the games operations, responsible for deterrence and detection of ML/TF/CPF risks – **Compliance Officer**

The Financial Intelligence Unit Curacao, referred to in art. 2 of the Norut – **FIU**

Source of Funds/Wealth – **SOF/SOW**

Know Your Business – **KYB**

The United States – **US**

Office of Foreign Assets Control – **OFAC**

Ultimate Beneficial Owner – **UBO**

Know Your Customer – **KYC**

Customer Due Diligence – **CDD**

Counter Terrorism Financing – **CTF**

Enhanced Due Diligence – **EDD**

Politically Exposed Person – **PEP**

Anti-Money Laundering – **AML**

The Caribbean Financial Action Taskforce (an organization of 24 states of the Caribbean Basin, Central and South America) – **CFATF**

Board of Directors of the Company – **BoD**

The National Ordinance on Offshore Games of Hazard (Landsverordening buitengaatsse hazardspelen, P.B. 1993, no. 63) – **NOOGH**

The European Union – **EU**

The United Nations – **UN**

Financial Action Task Force – **FATF**

The United Kingdom – **UK**

Money Laundering

The act of hiding or masking money obtained through illegal means, typically broken down into three phases: placement (introducing illicit money into the system), layering (obscuring the

money's origins through complex transactions), and integration (legitimizing the funds by reintroducing them into the economy).

AML Policy

A strategy aimed at curbing money laundering and terrorism financing, consisting of written internal policies, procedures, and safeguards. It is managed by an AML team, headed by a Money Laundering Reporting Officer (MLRO), who ensures the team receives proper training and organizes external audits of the program.

Anti-Money Laundering and Counter-Financing of Terrorism Program

A set of internal measures and controls to prevent both money laundering and terrorism financing, supervised by the AML team led by the MLRO. This person is responsible for ensuring AML-related training and auditing the program's effectiveness.

Money Laundering Reporting Officer (MLRO)

The person in charge of overseeing anti-money laundering efforts, including filing reports on suspicious transactions and enforcing AML policies and strategies within the organization.

Alert

A signal that prompts further review, triggered by certain predefined red flags or patterns, indicating potential money laundering or suspicious activity.

Beneficial Owner

The individual who has ultimate control or ownership of an account, even if it is managed by another party.

Blacklist

A list of individuals, organizations, or countries flagged for potential sanctions violations. This list is used for compliance purposes and may include internal, government, or vendor-maintained data.

Comprehensive Sanctions

Sanctions that prohibit all forms of interaction or transactions with a specific country, with very few exceptions.

Criminal Proceeds

Assets or funds that are obtained as a direct or indirect result of criminal activities.

Customer

Any individual or entity that opens an account and engages in business transactions with the Company.

Customer Relationship

All interactions between a customer and the Company from the point of onboarding through the entire lifecycle of the customer's engagement with the Company's products or services.

Know Your Customer (KYC)

A process involving the verification of a customer's identity and financial behavior, aimed at detecting unusual or suspicious activities.

Know Your Employee (KYE)

Policies to scrutinize employees to identify conflicts of interest, criminal backgrounds, or suspicious behavior that could pose risks to the company.

Due Diligence

A process of investigation and assessment of a person or entity before entering into a business relationship to ensure no legal, financial, or reputational risks are involved.

Customer Due Diligence (CDD)

Standard internal practices to confirm a customer's identity and evaluate their risk profile. It helps the company ensure compliance with regulations and mitigate risks like fraud and money laundering.

Enhanced Due Diligence (EDD)

Additional scrutiny applied to higher-risk customers, going beyond standard CDD procedures to gain a deeper understanding of their business activities and financial transactions.

High-Risk Third Country

Countries that are flagged by regulatory bodies like the European Commission or FATF due to insufficient measures to prevent money laundering or terrorism financing, thus posing significant risks.

Economic Sanctions

Measures imposed by one or more nations to influence another nation's policies, usually in the form of trade or financial restrictions.

Mandatory Sanctions Lists

Official lists required by law or regulation for organizations to check against when conducting business, such as UN Security Council Resolutions or local sanctions lists.

Egmont Group of Financial Intelligence Units

A global network of financial intelligence units (FIUs) that facilitates cooperation, training, and information-sharing to combat money laundering and terrorist financing.

Embargo

A government-imposed ban on trade or commercial activity with a specific country or product category.

European Union (EU)

A political and economic union of European countries that, among other things, sets regulations for combatting money laundering and terrorism financing across its member states.

Exclusions List

A list maintained by the compliance team containing names that have been cleared and excluded from further sanctions screening.

Financial Action Task Force (FATF)

An international organization that sets global standards for combating money laundering and terrorist financing. It also produces reports on emerging risks and trends in these areas.

Greylist

A list of countries or entities that have been identified as having weak anti-money laundering frameworks, but are working to address deficiencies.

Financial Intelligence Unit (FIU)

A national agency responsible for receiving and analyzing reports of suspicious financial transactions and forwarding them to the appropriate authorities.

First Line of Defense

The initial level of an organization's compliance framework, consisting of employees who interact directly with customers and gather relevant information to ensure proper screening.

Inherent Risk

The level of risk present before any mitigating measures or controls have been applied.

Investigation

The process of examining and gathering information in response to potential violations of sanctions or financial crimes.

Layering

A phase in the money laundering process where illicit funds are moved through various transactions to obscure their origins.

Minor

An individual under the age of 18.

Monitoring

The ongoing review of customer activity to detect unusual patterns or behavior, often aided by automated systems.

Office of Foreign Assets Control (OFAC)

A US Treasury Department agency responsible for administering and enforcing economic sanctions against foreign nations, organizations, and individuals.

Politically Exposed Person (PEP)

An individual in a prominent public position, such as a government official, whose financial transactions may require closer scrutiny due to the potential for corruption or illicit activities.

Red Flag

A warning sign indicating potential suspicious behavior or transactions that warrant further investigation.

Regulatory Agency

A governmental body responsible for overseeing financial institutions, issuing regulations, and enforcing compliance with laws.

2. Statement of the Policy

CAECUS N.V. is dedicated to preventing money laundering and the financing of terrorism through the establishment of this comprehensive AML/CTF/CPF Policy. This policy is aligned with both local and international standards to ensure compliance with all relevant regulations.

The primary objective of this policy is to create a robust framework for managing risks associated with various aspects, including customer interactions, service offerings, payment methods, geographical considerations, and distribution channels.

The Board of Directors (BoD) at CAECUS N.V. holds the responsibility for the approval and implementation of the policy, ensuring that it is effectively executed and monitored for compliance. This policy undergoes an annual review and may be revised as necessary to incorporate significant changes in regulations or operational procedures. Additionally, urgent amendments may be proposed by a designated officer based on recommendations from internal and external AML audits, taking into account any potential risks and impacts.

The AML/CTF/CPF Policy adheres to key legislation in Curacao, which includes the National Ordinance for Games of Chance (LOK), the Criminal Code of Curacao, the National Ordinance on Offshore Games of Hazard (NOOGH), the National Ordinance Penalization of Money Laundering (NOPML), the National Ordinance on the Reporting of Unusual Transactions (NORUT), and the National Ordinance on Identification when Rendering Services (NOIS), effective from May 16, 2024. The policy also complies with the Sanctions National Ordinance (SNO) and the Kingdom Sanction Act.

In addition to local legislation, this policy incorporates international standards and frameworks, such as the Financial Action Task Force (FATF) Recommendations, the European Anti-Money Laundering Directives (4th, 5th, and 6th AMLDs), and the Wolfsberg Principles.

CAECUS N.V. is committed to upholding the standards established by Curaçao's AML/CTF/CPF supervisory authority, the Curaçao Gaming Control Board. All directors, officers, and employees, along with any external consultants engaged for audit purposes, are required to follow and support the principles outlined in this policy.

3. Overview of the Online Gaming Environment

CAECUS N.V., a legally registered entity in Curaçao (Company Number 163779), operates the website <https://1xbet.com/en>. The company is authorized under the license issued by the Curaçao Gaming Control Board to offer games of chance (License Number OGL/2024/1262/0493), identified as, and adheres to the relevant licensing regulations and regional limitations set forth by the Curaçao regulatory authorities. These regulations prohibit remote gaming licensees from providing services to individuals in specific jurisdictions, including the United States, Australia, Dutch West Indies (Aruba and Bonaire), Curaçao, France, Germany, the United Kingdom, Belize, and the Netherlands. Consequently, CAECUS N.V. focuses its operations exclusively in markets where online gambling is permitted by law and refrains from targeting customers in regions where it is not allowed.

As an e-gaming and betting operator, CAECUS N.V. faces several potential risks related to money laundering. These risks encompass identity theft, fraud, the structuring and layering of transactions, and the possibility of collusion between employees, customers, or external payment service providers aiming to circumvent internal security protocols.

4. Understanding Money Laundering & Terrorism Financing

Money laundering represents a crucial aspect of financially motivated crime that frequently crosses international borders. It is associated with a range of illicit activities, including tax evasion, sanction violations, fraud, corruption, illegal arms trafficking, drug smuggling, extortion, and kidnapping. The primary objective of money laundering is to hide the illegal origins of the proceeds derived from these activities by disguising their identity, source, and intended use.

Stages of Money Laundering

The money laundering process typically unfolds in three distinct stages:

1. **Placement:** This initial step involves injecting illicit funds into the financial system. Common techniques include depositing cash into bank accounts, acquiring valuable assets, or engaging in various financial transactions. The aim is to start blending these funds into the legitimate economy.
2. **Layering:** In this stage, the illicit funds undergo a series of convoluted transactions to obscure their original source. This can involve transferring money between multiple accounts, exchanging currencies, or investing in diverse financial products. The objective is to create a complex network of transactions that obscures the audit trail, making it challenging to trace the money back to its origin.
3. **Integration:** The final stage involves reintegrating the laundered money into the legitimate economy. This can be achieved by purchasing high-value items, investing in

cash-intensive businesses, or participating in other legal financial activities. At this point, the funds appear legitimate and are significantly more difficult to link back to their illegal origins.

Money laundering can occur at various points within this process, and online gambling platforms can be susceptible to misuse during these stages. This emphasizes the necessity for CAECUS N.V. to avoid providing anonymous services or facilitating dubious transactions.

Relationship to Terrorist Financing

Terrorist financing entails the funds used to support terrorist activities. These funds may originate from legitimate sources but are often funneled through financial systems in a manner akin to money laundering. For instance, prepaid cards are often employed to procure materials for terrorist acts. Therefore, it is essential for staff to receive training on current developments in this field.

Risk Management and Compliance Strategies

To mitigate the threats posed by money laundering, CAECUS N.V. prioritizes the identification and management of potential risks. Key strategies include:

- Performing comprehensive customer due diligence to confirm identity documentation, age, and location, addressing issues of fraud and identity theft.
- Vigilantly monitoring for unusual patterns of activity involving multiple accounts or significant transaction volumes to detect irregularities.
- Identifying and addressing deposits originating from illicit activities or used to temporarily hold such funds within the platform.
- Observing player-to-player transfers to prevent misuse of the platform for transferring funds between individuals or cashing out.

This list is not exhaustive, as new risks may arise. The company conducts regular risk assessments tailored to specific concerns and offers ongoing training to employees to enhance its internal anti-money laundering (AML) compliance initiatives.

Terrorism financing encompasses the provision of funds intended to support terrorist activities, sourced from both legal and illegal means. These funds are crucial for executing a range of operations related to terrorism.

The sources of terrorist funding can be divided into two categories: legal and illegal. Legal sources may include legitimate businesses, charitable donations, and lawful financial activities, which terrorists can exploit to channel money through donations and business transactions. In contrast, illegal sources stem from criminal activities such as drug trafficking, fraud, smuggling, and extortion, alongside money laundering tactics that obscure the origins of the funds.

Funds are transferred through a variety of methods. Formal channels involve traditional banking systems and financial institutions, where sophisticated techniques like layering and structuring are utilized to avoid detection. Alternatively, informal channels, such as hawala systems, operate outside regulated financial frameworks, making them more difficult to trace.

Indicators of terrorism financing often manifest as unusual transaction patterns that diverge from standard personal or business behavior. This may include large or frequent transfers to or from high-risk regions and transactions associated with known terrorist affiliates. Furthermore, suspicious activities can surface in high-risk sectors, involving substantial cash transactions or financial actions seemingly designed to conceal terrorist operations.

To effectively combat terrorism financing, robust regulatory and compliance measures are vital. The Anti-Money Laundering (AML) policies of CAECUS N.V. are specifically structured to identify and prevent such activities through customer due diligence (CDD), transaction monitoring, and the reporting of any suspicious activities. The company adheres to various sanctions lists, including but not limited to the Sanctions National Ordinance (SNO, N.G. 2014, no. 55), the Kingdom Sanction Act (N.G. 2016, no. 54), announcements from the Gaming Control Board (GCB), the Office of Foreign Assets Control (OFAC), United Nations Security Council sanctions, EU sanctions, and the U.S. List of Foreign Terrorist Organizations. These lists help ensure that transactions do not inadvertently support terrorism.

Internationally, the Financial Action Task Force (FATF) provides guidelines aimed at addressing money laundering and terrorism financing, stressing the importance of robust policies for detecting and reporting suspicious transactions. The OFAC enforces U.S. economic and trade sanctions and maintains the Specially Designated Nationals (SDN) list, which includes individuals and entities linked to terrorism. The European Union (EU) also enforces regulations designed to prevent the financial system from being misused for terrorist purposes, requiring member states to implement effective AML measures and adhere to international sanctions. Moreover, the United Nations (UN) contributes to global efforts to disrupt terrorist financing by imposing sanctions and maintaining lists of individuals and entities connected to terrorism, thereby limiting the resources available to terrorist groups.

5. Assessment of Risks Related to Money Laundering, Terrorist Financing, and Proliferation Financing

CAECUS N.V. adopts a comprehensive risk-based approach (RBA) to effectively implement its Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF) and Counter-Proliferation Financing (CPF) strategies. This methodology is essential for prioritizing resources toward mitigating the most significant threats. The recent revisions in Curaçao's gaming regulations, particularly with the introduction of the new Law on Offshore Games (LOK), necessitate a robust RBA for compliance and to preserve the integrity of the gaming sector.

The LOK, which replaces the previous National Ordinance on Offshore Games of Hazard (NOOGH), imposes enhanced requirements regarding AML/CTF/CPF for gaming operators. This legislation mandates that operators conduct thorough risk assessments to identify and understand the specific vulnerabilities that their operations may encounter. Consequently, CAECUS N.V. must evaluate various factors, including customer demographics, transaction

patterns, geographic locations, and the nature of the services offered, to determine the level of risk associated with money laundering and terrorist financing.

Moreover, the RBA requires continuous monitoring and the adoption of effective internal controls. Operators are expected to develop and implement policies that not only comply with Curaçao's regulations but also align with international standards set by the Financial Action Task Force (FATF) and relevant European Union (EU) directives. These guidelines emphasize the importance of identifying and mitigating risks associated with specific products and services that may be susceptible to exploitation by criminals.

In addition to local legislation, CAECUS N.V. is also bound by international regulations that govern financial integrity and security. The FATF provides recommendations that aim to prevent the misuse of the financial system for illegal activities, including money laundering and terrorist financing. Compliance with these recommendations involves establishing a strong framework for customer due diligence (CDD), transaction monitoring, and reporting suspicious activities.

Furthermore, the European Union has enacted a series of Anti-Money Laundering Directives (4th, 5th, and 6th AMLDs) that require member states to implement stringent measures to combat money laundering and terrorist financing. As a jurisdiction linked to the EU, Curaçao must align its regulatory framework with these directives to ensure its gaming operators meet high standards of accountability and transparency.

The recent developments in Curaçao's gaming regulations reflect a broader international effort to address the risks of proliferation financing as well. The company must remain vigilant against attempts to finance activities related to the proliferation of weapons of mass destruction, which can be intertwined with the risks of money laundering and terrorist financing. By adhering to international sanctions and regulations, including those imposed by the United Nations Security Council and the Office of Foreign Assets Control (OFAC), CAECUS N.V. ensures that it does not inadvertently facilitate transactions linked to prohibited individuals or entities.

In conclusion, the implementation of a comprehensive risk-based approach is vital for CAECUS N.V. to navigate the complexities of money laundering, terrorist financing, and proliferation financing. By integrating local regulations with international standards, the company not only enhances its compliance framework but also strengthens its reputation within the global gaming industry.

5.1. Fundamental Elements of the Risk-Based Strategy

A fundamental component of CAECUS N.V.'s RBA is its detailed risk assessment process, which systematically examines risks across various facets including customer profiles, products and services offered, and the geographical areas of operation. This comprehensive assessment is conducted on a regular basis to identify vulnerabilities that could be exploited.

In evaluating customer risk, the company considers several factors, such as the presence of politically exposed persons (PEPs), the geographical origin of customers, and the complexity of their business structures. Product and service risks are similarly assessed, focusing on offerings that involve high transaction volumes or facilitate anonymity. Additionally, geographical risk is

determined by evaluating the locations of customers and business activities, particularly in jurisdictions that exhibit weak AML/CTF/CPF frameworks or high corruption levels.

Once risks are identified, CAECUS N.V. tailors its mitigation strategies to suit the severity of the risks involved. This includes implementing enhanced due diligence (EDD) measures, utilizing sophisticated transaction monitoring systems, and establishing rigorous customer verification procedures. EDD involves collecting additional data on high-risk clients and transactions, such as verifying the source of funds and identifying beneficial owners. The company employs advanced transaction monitoring systems that are designed to flag suspicious activities through established alert thresholds and by analyzing transaction patterns indicative of potential illicit activities.

Continuous oversight and periodic reviews are essential to the RBA's success. CAECUS N.V. consistently evaluates transaction data to spot unusual activities, updates customer profiles with relevant new information, and adjusts its AML/CTF/CPF policies and procedures to remain in line with evolving regulatory standards and risk landscapes.

Accurate reporting mechanisms and diligent record-keeping practices are vital components of the RBA framework. The company ensures that all identified suspicious transactions are reported to the appropriate authorities without delay. Furthermore, comprehensive records related to customer identification, transaction histories, and risk assessments are meticulously maintained for the legally mandated retention period. These records are readily accessible for regulatory review and inspections.

5.2. Adherence to Curaçao's Legislation

In compliance with the newly established Law on Offshore Games (LOK), CAECUS N.V. actively develops and implements robust AML/CTF/CPF programs that integrate the principles of the RBA, tailored to the organization's size, nature, and operational complexity. To ensure that employees are well-equipped to fulfill their AML/CTF/CPF responsibilities, regular training is provided, with a focus on understanding the RBA and effective risk management practices. Independent audits are also conducted to evaluate the effectiveness of the AML/CTF/CPF programs and the application of the RBA across the organization.

5.3. Unique Risks Associated with the Gambling Sector

The gambling industry is marked by distinct risk factors that CAECUS N.V. is committed to addressing. The assessment of customer risk involves identifying potential vulnerabilities related to various individuals. Particular attention is given to individuals with irregular income sources, those categorized as PEPs, and high spenders whose financial behavior seems disproportionate to their known resources. To mitigate these risks, the company employs thorough customer due diligence (CDD), including EDD for high-risk individuals, consistent updates of customer profiles, and strict identity verification processes. Additionally, third-party transactions are limited and only allowed when thoroughly verified.

Geographical risk evaluation focuses on assessing the potential dangers linked to the origin of a player's funds and their physical locations. Countries deemed high-risk often possess weak

AML/CTF/CPF systems or exhibit considerable corruption. To manage these geographical risks, CAECUS N.V. continuously monitors and assesses countries based on their risk profiles, updating geographical assessments using credible intelligence, and applying stricter due diligence measures for customers from high-risk regions.

The gaming sector inherently carries product, service, and transaction risks, rendering it susceptible to criminal exploitation. High-risk factors include the handling of illicit funds, anonymous virtual assets, or prepaid cards. CAECUS N.V. addresses these challenges by implementing stringent client identity verification protocols, ensuring that funds are sourced only from licensed providers, closely monitoring casino accounts and peer-to-peer transactions, and employing advanced fraud detection mechanisms. Staff training and the proactive reporting of suspicious activities further reinforce the company's risk management strategy.

Distribution channel risks pertain to the channels utilized to establish business relationships. The use of anonymous channels and non-face-to-face interactions elevates the risk of identity theft and fraud. Additionally, third-party intermediaries, especially those not bound by AML/CTF/CPF regulations, pose extra threats. To mitigate these risks, CAECUS N.V. employs advanced tools for client identity verification, thwarts impersonation attempts, and ensures that no anonymous or unregulated third parties are engaged in customer interactions.

By incorporating a comprehensive risk-based approach within its AML/CTF/CPF policies, CAECUS N.V. effectively confronts the risks associated with money laundering and terrorist financing. This commitment not only ensures compliance with Curaçao's updated regulations but also promotes the overall integrity of the gaming industry.

6. Customer Due Diligence

The company is dedicated to maintaining compliance with regulatory standards that prohibit the establishment of anonymous or fictitious accounts within the casino sector. To effectively combat risks related to money laundering, terrorist financing, and proliferation, it is imperative to verify player identities and comprehend their business relationships. A comprehensive Customer Due Diligence (CDD) policy is essential for evaluating risks and ensuring adherence to all regulatory obligations. Any activities deemed suspicious will be reported to the Financial Intelligence Unit (FIU) and, if necessary, to the Public Prosecutor's Office.

6.1. Conditions for Implementing CDD Measures

The company will implement CDD measures under the following conditions:

- **Transactions of NAF 4,000 or more:** CDD measures are applied to any single transaction that meets or exceeds this threshold.
- **Occasional transactions exceeding NAF 4,000:** This includes infrequent transactions that surpass the specified limit.

- **Suspicion of illicit activities:** Any indication of money laundering or terrorist financing will trigger CDD protocols.
- **Uncertainties in customer identification:** If previously obtained identification data raises doubts, CDD measures will be activated.
- **Linked transactions:** This applies to either a single transaction or multiple transactions that collectively exceed NAF 4,000. Even if individual transactions are below this threshold, linked transactions will still necessitate CDD. High-risk transactions will require Enhanced Due Diligence (EDD).

6.2. Components of the CDD Process

The company's CDD procedures will encompass the following actions:

- **Identity Verification:** Players will be identified using credible, independent documents or data. This process includes confirming the ultimate beneficial owner of legal entities and understanding their ownership structure.
- **Ongoing Monitoring:** Continuous due diligence will be conducted to monitor transactions, ensuring alignment with the company's understanding of the player and their risk profile, including the source of funds as needed.
- **Confidential Reporting:** Employees are instructed to maintain confidentiality regarding reports made to the FIU, thereby preventing players from being alerted. If suspicions of money laundering or terrorist financing arise, the company will bypass standard CDD processes and report directly to the FIU.

6.3. Player Identity Establishment

To establish a player's identity, the following information will be collected:

- Full name
- Permanent residential address
- Date of birth
- Place of birth
- Nationality
- Identity number

For low-risk scenarios, only basic information will be required. In higher-risk situations, more detailed information will be collected to mitigate the risks associated with money laundering and terrorist financing.

- **Risk Evaluation:** Players will be assigned initial risk ratings based on collected information, which will be revised as more data becomes available to determine the appropriate level of CDD.
- **Verification Methods:** Identity verification will be executed through:
 - Government-issued photo identification (e.g., passport or ID card).
 - Supplementary documents (e.g., utility bills or bank statements) confirming the address, dated within the last six months.

- Verification of the address through communication methods such as letters, email, or phone.
- Biometric checks, cross-referencing database information, IP addresses, and funding methods.

If initial information is insufficient, further verification steps may include requesting a selfie with the ID or confirming the first deposit through a regulated financial institution.

6.4. Understanding Player Relationships

The company will seek to identify the purpose and nature of its relationships with players as part of the CDD process. While some relationships may be clear, the company will gather sufficient information to detect any unusual or suspicious activities. For higher-risk clients, detailed documentation of their source of wealth and expected activity levels will be collected to ensure legitimacy. For lower and medium-risk players, basic employment or business information will suffice, supplemented by independent verification for higher-risk individuals.

6.5. Continuous Surveillance

The company's AML/CTF/CPF policy mandates ongoing surveillance of player identities and transactions. This includes:

- **Regular Updates:** Player details will be routinely verified, especially for high-risk individuals.
- **Transaction Scrutiny:** Transactions will be closely examined for unusual patterns.
- **Enhanced Due Diligence:** Transactions meeting or exceeding NAF 4,000 will be subjected to enhanced scrutiny, including linked transactions.

Advanced monitoring systems will be utilized to identify potential red flags in real-time, facilitating prompt investigations and reports to the FIU.

6.6. Enhanced Investigation for High-Risk Cases

In high-risk scenarios, the company will apply Enhanced Due Diligence (EDD) measures, which include:

- Comprehensive investigations into the player's background.
- Verification of sources of funds and wealth.
- Detailed examinations of transaction patterns.
- Regular updates of identification information.

EDD measures will be particularly relevant for politically exposed persons (PEPs), necessitating thorough risk assessments and continuous monitoring.

6.7. Simplified Verification for Low-Risk Cases

For low-risk scenarios, Simplified Due Diligence (SDD) measures will be implemented, which involve gathering basic customer information and conducting less frequent reviews. Although

SDD streamlines the process, enhanced measures will be enacted if suspicious activities arise or if the player's risk profile changes.

6.8. Special Considerations for Politically Exposed Persons (PEPs)

The company's AML/CTF/CPF policy will require heightened scrutiny of PEPs, their family members, and close associates. EDD measures for these individuals will include obtaining senior management approval, understanding the source of funds and wealth, and conducting rigorous ongoing monitoring.

6.9. Relationship Termination Protocol

The company reserves the right to terminate relationships with players engaged in suspicious activities or those who fail to provide sufficient information. Such decisions must be documented and approved by senior management. Upon termination, all activities will be reviewed, and any suspicious transactions will be reported to the FIU. Records related to terminated relationships will be securely stored for a minimum of five years.

7. Sanctions Compliance

The company is firmly committed to adhering to both international sanctions and regulatory standards as part of our Anti-Money Laundering, Counter-Terrorist Financing, and Proliferation Financing (AML/CTF/CPF) policy. To fulfill these obligations, we have established comprehensive procedures designed to ensure compliance with all sanctions imposed by national and international authorities. This includes conducting thorough due diligence on every client and transaction to prevent any interactions with sanctioned individuals, entities, or regions.

7.1. Monitoring and Reporting Procedures

Monitoring and reporting are vital components of our sanctions compliance efforts. The company continuously scrutinizes all transactions for any suspicious activities that could violate sanctions. Any irregularities identified will be promptly reported to the appropriate authorities. Additionally, our commitment to compliance is bolstered by ongoing training for all personnel, ensuring that they remain informed about current sanctions regulations. This proactive approach helps safeguard our operations and mitigate potential risks associated with sanctions violations.

7.2. Client Interaction and Transaction Verification

To maintain the integrity of our operations, all client interactions and transactions undergo meticulous checks against the latest Sanctions Lists. Automated systems facilitate real-time verifications, and our database is regularly updated to reflect current sanctions information. If a match or suspicious activity is detected, it will be reported immediately to the relevant authorities. The company will take decisive actions, including freezing accounts or blocking transactions, to manage compliance risks effectively.

7.3. Continuous Review of Compliance Procedures

Our sanctions compliance procedures are subject to regular reviews and updates to align with evolving legislation and best practices. This includes ongoing monitoring of the following lists:

- Sanctions National Ordinance (SNO, N.G. 2014, no. 55)
- Kingdom Sanction Act (N.G. 2016, no. 54)
- GCB announcements
- EU Sanctions
- UK OFSI Sanctions
- UN Security Council Consolidated List
- US List of Foreign Terrorist Organizations
- OFAC Sanctions

7.4. Due Diligence and Evasion Prevention

Our due diligence efforts are specifically designed to uncover any indirect or covert attempts to engage with sanctioned parties or jurisdictions. If any evasion tactics are identified, they will be reported immediately to the relevant authorities, and corrective actions—including transaction suspensions and account reviews—will be implemented without delay.

7.5. Staff Training and Auditing

Regular audits and continuous training for staff are critical to ensuring that the company remains vigilant and compliant with the latest legislative requirements. This ongoing education helps reinforce our commitment to preventing sanctions evasion and maintaining a robust compliance framework.

8. Management Responsibilities

Senior management plays a crucial role in assessing and managing the risks associated with Anti-Money Laundering, Counter-Terrorist Financing, and Proliferation Financing (AML/CTF/CPF) within the company. To ensure effective oversight, the Board of Directors mandates that the appointed AML/CTF/CPF Officer provides regular updates regarding significant changes or challenges within the control environment. This officer is also responsible for preparing an annual report that evaluates the effectiveness of the company's measures and controls aimed at mitigating risks related to money laundering, terrorist financing, and proliferation financing.

8.1. Policy Review and Risk Assessment

Senior management is accountable for conducting comprehensive reviews of all relevant policies and procedures at least once each year. These reviews are guided by monthly risk assessments, enabling the identification and timely addressing of any potential vulnerabilities in internal

controls and risk management practices. If any deficiencies are identified, the AML/CTF/CPF Officer can recommend necessary adjustments to the Board for approval, thus enhancing the company's risk management and compliance framework.

8.2. Employee Training Programs

In alignment with global best practices, senior management is responsible for overseeing the creation and execution of extensive employee training programs. These initiatives are designed to increase awareness and understanding of AML/CTF/CPF risks among all employees, especially those in critical roles, ensuring they are equipped to effectively recognize and respond to suspicious activities.

8.3. Internal Control Framework

Senior management also ensures that the company maintains a robust internal control framework. This includes establishing adequate segregation of duties, implementing clear authorization processes, conducting ongoing monitoring, and ensuring thorough documentation. To uphold regulatory compliance and enhance the effectiveness of the AML/CTF/CPF program, regular independent audits and assessments are performed to provide objective evaluations and identify areas for improvement.

9. Compliance Officer

9.1. Designation and Authority

The company appoints a qualified individual to serve as the Compliance Officer, a key element of our Anti-Money Laundering (AML) strategy. This appointment is made by senior management to guarantee the role's independence and authority. The Compliance Officer possesses extensive expertise in AML compliance and occupies a senior position, enabling them to effectively oversee the implementation of AML policies and procedures. Their role is formally established through an appointment letter outlining their responsibilities and the organizational reporting structure.

9.2. Key Functions of the Compliance Officer

The Compliance Officer is tasked with several critical functions to ensure the effectiveness of our AML program. These primary duties include:

- **Policy Implementation:** Overseeing the execution of AML policies and procedures to ensure alignment with current regulations.
- **Central Point of Contact:** Serving as the main contact for all AML-related issues.
- **Policy Review:** Regularly reviewing and updating AML policies to address evolving regulatory standards and emerging risks.

- **Training Oversight:** Managing the AML training program to ensure employees are adequately informed about AML requirements and their roles in maintaining compliance.

9.3. Core Responsibilities

The Compliance Officer is entrusted with several essential responsibilities:

- **Transaction Monitoring and Reporting:** Continuously analyzing transactions and client activities to identify suspicious behavior. They are responsible for filing Suspicious Activity Reports (SARs) with the Financial Intelligence Unit (FIU) when necessary and maintaining accurate records of these reports.
- **Policy Development and Updates:** Crafting and revising AML policies and procedures to adhere to the latest Curaçao gaming regulations and international best practices. This includes adapting the AML framework to address new risks and regulatory changes.
- **Employee Training and Awareness:** Ensuring that all staff receive comprehensive AML training and understand their responsibilities in detecting and reporting suspicious activities. The Compliance Officer must regularly update training materials to reflect legislative or policy changes.
- **Regulatory Liaison:** Acting as the primary contact with regulatory bodies, law enforcement, and other relevant authorities on AML matters. This includes responding to information requests and participating in regulatory inspections or audits.
- **Compliance Audits:** Conducting regular reviews and audits of the AML program to evaluate its effectiveness and compliance with legal requirements. The Compliance Officer is responsible for addressing any identified issues and implementing necessary corrective measures.
- **Record-Keeping:** Maintaining detailed records of all AML-related activities, including SARs, internal reports, training sessions, and policy updates. These records must comply with legal requirements and be readily available for regulatory review.

9.4. Conclusion

Through the execution of these functions and responsibilities, the Compliance Officer plays a vital role in safeguarding the organization against money laundering and terrorist financing risks, ensuring rigorous compliance with Curaçao's AML regulations.

10. Detection and Reporting of Suspicious Activity

CAECUS N.V. is committed to recognizing and reporting any suspicious activities that may suggest possible money laundering or terrorist financing. Such activities may include unusual patterns in a client's behavior, frequent high-value transactions, or interactions with high-risk jurisdictions. All employees are encouraged to be vigilant and promptly report any irregularities to the designated Compliance Officer, who will conduct a comprehensive investigation to determine if further action or reporting to the appropriate authorities is necessary.

10.1. Characteristics of Unusual Transactions

Unusual transactions are identified by marked departures from a client's typical business practices or financial profile. Examples may include unexpectedly large transactions, dealings with unknown entities, or transactions that lack a legitimate economic or lawful purpose. Employees use transaction monitoring systems to detect these anomalies and escalate them to the Compliance Officer for further analysis.

10.2. Assessment and Reporting Procedures

Upon receiving reports of unusual transactions, the Compliance Officer will evaluate these activities against established risk indicators and legal standards to ascertain whether they are suspicious. If warranted, the Compliance Officer will submit a report to the Financial Intelligence Unit (FIU) in accordance with Curaçao's anti-money laundering regulations.

10.3. Confidentiality of Reporting Process

To uphold the integrity of the reporting process and comply with legal mandates, CAECUS N.V. enforces a strict policy prohibiting the disclosure of any information pertaining to Suspicious Activity Reports (SARs) to the subjects of these reports or to unauthorized individuals. This confidentiality is essential to prevent any interference with ongoing investigations or legal proceedings. Employees are required to handle all communications regarding SARs with utmost discretion, discussing such matters only with the Compliance Officer or authorized personnel. Any violation of this confidentiality policy is regarded as a serious breach of the company's anti-money laundering framework and may lead to disciplinary actions. This rigorous policy ensures that the reporting process remains confidential and effective in mitigating potential risks to the organization.

11. Audit Procedures

To comply with the updated gaming regulations in Curaçao, CAECUS N.V. conducts an independent audit focused on Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF). This section details the audit process, highlighting the responsibilities of the independent auditor and the review conducted by the Gaming Control Board.

11.1. Objectives of the Audit

The primary aim of the annual AML/CTF/CPF audit is to evaluate the effectiveness and compliance of the company's AML/CTF/CPF practices. This audit is crucial for ensuring adherence to current legal standards and best practices designed to mitigate risks related to money laundering and terrorist financing. The audit encompasses a thorough examination of the AML/CTF/CPF program, which includes risk assessments, transaction monitoring, staff training, and reporting procedures.

11.2. Auditor Appointment

CAECUS N.V. appoints either an external auditor or an internal audit team with the necessary resources and expertise in AML/CTF/CPF. To avoid any conflicts of interest, this auditor operates independently from the company's AML Compliance team. The company carefully assesses the auditor's credentials, experience, and industry reputation. Additionally, the selected auditor must receive approval from the Gaming Control Board to ensure compliance with Curaçao's gaming regulations.

11.3. Adherence to Standards

The audit process follows international standards and specific requirements set forth by the Gaming Control Board. Key elements of the audit process include:

- **Evaluation of AML/CTF/CPF Policies and Procedures:** Confirming that policies are up-to-date and compliant with legal standards.
- **Risk Management Assessment:** Analyzing the effectiveness of risk assessments and mitigation strategies.
- **Transaction Monitoring Review:** Evaluating the efficiency of systems used to detect and report suspicious activities.
- **Staff Training Evaluation:** Assessing the adequacy and effectiveness of employee training programs.
- **Reporting Mechanism Audit:** Reviewing procedures for reporting suspicious transactions and compliance issues.
- **Customer File Review:** Ensuring adherence to KYC (Know Your Customer), KYB (Know Your Business), and CDD (Customer Due Diligence) protocols.

11.4. Audit Reporting

Following the audit, the independent auditor prepares a detailed report summarizing their findings, recommendations, and any issues identified. This report is submitted to the company's senior management and the Gaming Control Board. CAECUS N.V. is committed to addressing the auditor's recommendations and implementing corrective actions within an established timeframe. Follow-up audits may be required to ensure that corrective measures are effectively executed.

11.5. Oversight by the Gaming Control Board

The Gaming Control Board oversees AML/CTF/CPF compliance for all licensed operators, including reviewing audit results and conducting its evaluations. CAECUS N.V. understands that the Board has the authority to request additional documents, perform inspections, and review the implementation of audit recommendations.

11.6. Consequences of Non-Compliance

The company acknowledges that non-compliance identified through audit results or Board evaluations may lead to penalties, including fines, operational restrictions, or even the

suspension or revocation of its gaming license. Therefore, CAECUS N.V. is dedicated to collaborating closely with the Gaming Control Board to implement corrective actions and maintain compliance, thereby preventing future complications.

12. Record Keeping

To adhere to stringent record-keeping standards, our company implements robust procedures for managing documentation associated with AML/CTF/CPF. We maintain comprehensive records, which include customer identification information, transaction details, suspicious activity reports (SARs), training logs, and audit records, all preserved for a minimum of five years.

We ensure the security of these records through advanced encryption techniques and strict access controls to prevent unauthorized access. Regular audits are conducted to verify the integrity of the data and safeguard against potential breaches.

A systematic approach is adopted for organizing records, allowing for efficient retrieval by authorized personnel and regulatory bodies. We conduct continuous internal monitoring and periodic audits to ensure compliance with established protocols.

By effectively managing our records, the company not only meets regulatory requirements but also facilitates auditing processes and contributes to the overall integrity of the gaming industry.

13. Training

CAECUS N.V. has implemented a comprehensive training program focused on Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) for all employees. The primary objective of this training is to equip staff with the essential knowledge and skills needed to detect and prevent activities related to money laundering and terrorist financing. Employees are educated on their legal responsibilities, trained to identify suspicious behaviors, and familiarized with the reporting procedures. A well-informed workforce is crucial for effectively executing AML/CTF/CPF policies, which uphold the integrity and credibility of the gaming industry.

13.1. Role-Specific Training Requirements

The training is tailored to address the specific needs of different roles within the organization and is mandatory for all personnel, including senior management, compliance officers, customer-facing staff, and operational teams involved in financial transactions.

13.2. Training Structure

New employees undergo an extensive initial training program, while all staff members participate in refresher courses at least once a year. Employees in high-risk roles may receive additional training sessions more frequently to ensure they are adequately prepared.

13.3. Training Curriculum Content

The training curriculum covers essential topics, including:

- **AML/CTF/CPF Laws and Regulations:** Specific to Curaçao.
- **Internal Policies:** Overview of CAECUS N.V.'s policies and procedures.
- **Compliance Roles:** Understanding the roles employees play in maintaining compliance.
- **Customer Identification and Verification:** Including KYC (Know Your Customer) and CDD (Customer Due Diligence) processes.
- **Reporting Suspicious Activities:** Guidelines on identifying and reporting suspicious behaviors.
- **Record-Keeping Requirements:** Understanding documentation and record-keeping standards.
- **Implications of Non-Compliance:** Exploring the consequences of failing to comply.
- **Emerging Trends:** Keeping up with trends in money laundering and terrorist financing.

13.4. Delivery Methods

To ensure the training is engaging and effective, CAECUS N.V. utilizes various delivery methods, such as in-person workshops, online courses, interactive e-learning modules, and practical exercises like case studies and role-playing scenarios. This multifaceted approach accommodates different learning styles and reinforces key concepts.

13.5. Qualified Trainers

Training sessions are led by qualified professionals, including internal compliance officers and external consultants, to ensure that the content remains current and relevant, accurately reflecting the latest developments in AML/CTF/CPF compliance.



Capital Trust Corporation NV
Date: 11 November 2024