

A blue video game controller is positioned in the foreground, resting on a dark surface. The background is a blurred cityscape at night, with warm orange and yellow lights from buildings and streetlights creating a bokeh effect. The text is overlaid on the center of the image.

Grace Bay B.V.
Anti-Money Laundering,
Counter-Terrorist
Financing, Counter-
Proliferation Financing and
Sanctions Policy

Table of Contents

1-Introduction.....	7
1.1 About Grace Bay B.V.	7
1.2 Objective / Purpose	7
1.3 Application & Scope	8
1.4 Review Frequency.....	8
1.5 Definitions	9
1.6 AML Regulatory Framework.....	12
2.Risk Based Approach	15
2.1.1. Type of Customers and Their Activities	15
2.1.2. The Countries or Geographic Areas in Which the Company Does Business.....	15
2.1.3. Customer Risk Assessment	15
2.1.4. Transaction Risk Management	16
2.1.5. Services Risk (Product & Service Risk Factors).....	16
2.1.6. Geographical Risk and Jurisdictional Exposure.....	16
2.1.7. Cryptocurrency Risk Management.....	16
2.1.8. Delivery Channel Risk	17
2.1.9. Third-Party Risk.....	17
2.1.10. Ongoing Monitoring and Reporting.....	17
2.1.11. Commitment to Managing Transaction Risks	17
2.1.12. Mitigation Measures.....	17
2.1.13. Commitment to Security and Compliance	18
2.1.14. Commitment to Secure Delivery Channels.....	18
2.2. Risk Matrix for Likelihood and Impact	19
2.2.1. Risk Matrix for Likelihood and Impact for Grace Bay B.V.	19
2.2.2. Likelihood Assessment for Grace Bay B.V.	19
2.2.3. Impact Assessment for Grace Bay B.V.	19
2.2.4. Risk Matrix Application for Grace Bay B.V.	20
2.3. Risk Categories and Factors.....	20
2.3.1. Customer Risk.....	20
2.3.2. Geographical Risk.....	21
2.3.3. Transaction Risk.....	21
2.3.4. Product and Service Risk	21

2.3.5. Crypto-Specific Risk	22
2.3.6. Payment Method Risk	22
2.3.7. Behavior Risk.....	23
2.3.8. Compliance Risk	23
2.3.9. Reputational Risk	23
2.3.10. Operational Risk.....	24
2.3.11. Political and Legal Risk	24
2.4. Detailed Risk Matrix for Grace Bay B.V	24
2.4.1 Risk Level Summary:.....	26
3. Customer Due Diligence (CDD).....	28
3.1. CDD Objectives	28
3.2. When CDD is Required.....	28
3.3. CDD Procedures.....	28
3.3.1. Identification and Verification	28
3.3.2. Customer Risk Profiling.....	28
3.3.3. Ongoing Monitoring.....	29
3.4. Enhanced Due Diligence (EDD).....	29
3.5. Simplified Due Diligence (SDD)	29
3.6 Failure to Conduct Customer Due Diligence	29
3.7. Suspicious Activity Reporting (SAR)	30
3.8 Confirmation of Customer Onboarding and Service Providers	30
3.9 Structured diagram for Customer Onboarding Process.....	31
3.10 MLRO Responsibilities in Customer Onboarding	31
3.11. Record Keeping and Reporting	32
3.8. Training and Awareness	32
4. Know your Customer (KYC), Sanctions Screening, Transaction Monitoring and Reporting	34
4.1 Know Your Customer (KYC) System.....	34
4.1.1. Customer Onboarding and Identification Process.....	34
4.1.2. Risk-Based Approach for Customer Classification.....	34
4.1.3. Enhanced Due Diligence (EDD) for High-Risk Customers.....	35
4.1.4. Crypto-Specific KYC Measures	35
4.1.5. Ongoing Customer Monitoring and Re-verification	36

4.1.6. Geographical Risk Management	36
4.1.7 Customer KYC & Control Checks to Minimize Fraud Risk	36
Step 2: KYC Checks	38
4.1.8. Data Protection and Compliance with Global Privacy Laws	39
4.2. In-House Sanctions Screening System.....	39
4.2.1 Scope of the Sanctions Screening System.....	39
4.2.3 Objectives of Sanction Screening System.....	39
4.2.4 Key Components of the In-House Sanctions Screening System.....	39
4.2.4. Customer Onboarding & Registration Screening.....	40
4.2.3. Ongoing Transactional Screening	40
4.2.4. Risk-Based Approach for Screening of High-Risk Customers	40
4.2.5. Cryptocurrency-Specific Controls.....	41
4.2.6. Internal Reporting and Investigation.....	41
4.2.7. Ongoing Monitoring and Training	41
4.3 In-House Transactions Monitoring System.....	42
4.3.1. System Overview	42
4.3.2. Key Features of the Transactions Monitoring System	42
4.3.3. Alert System.....	43
4.3.4. AML Detection System.....	43
4.3.5. Crypto Risk Policies.....	44
4.3.6 Failure to Report Suspicious Activity & Suspicious Transaction	44
4.3.7 Tipping Off.....	44
5. Lines of Reporting & Record Keeping	46
5.1. Lines of Reporting.....	46
5.1.1. Reporting Procedures	46
5.2 Record Keeping.....	46
5.2.1. Customer Due Diligence (CDD) Records:.....	46
5.2.2 Transaction Records:	47
5.2.3 Suspicious Transaction Reports (STRs) & Suspicious Activity Reports (SARs):	47
5.2.4 Internal and External Audit Reports:.....	47
5.2.5 Communication Records:.....	47
5.2.6 Employee Training Records:.....	47
5.2.7. Data Security and Confidentiality	47

5.2.8. Disposal of Records	47
6. Training and Awareness.....	49
6.1. General Training Requirements.....	49
6.2 Training Frequency:	49
6.2. Training Content.....	49
6.3. Role-Specific Training	50
6.4. AML Awareness Campaigns	50
6.5. Evaluation and Continuous Improvement.....	51
6.6. Reporting and Documentation of Training	51



1. Introduction

1-Introduction

This Anti-Money Laundering (AML) policy outlines the comprehensive framework designed to prevent and detect money laundering (ML), proliferation financing (PF) and terrorist financing (TF) activities within Grace Bay B.V. as a global services provider. The policy is aligned with international AML standards, including the Curaçao Gaming Authority (CGA) regulations, and is tailored to address the risks associated with the company's worldwide remote gaming operations. Given the company's use of cryptocurrency and fiat transactions, this policy is applicable across all jurisdictions in which the company operates, ensuring a consistent and proactive approach to compliance as Grace Bay B.V. expands its global reach.

This policy will focus on regulatory compliance in all countries where Grace Bay B.V. operates, ensuring that the AML framework is flexible and robust enough to accommodate local regulations and the risks associated with different jurisdictions.

1.1 About Grace Bay B.V.

Grace Bay B.V. is a private limited liability company registered under the Curaçao Chamber of Commerce & Industry, incorporated under the laws of Curaçao with Company Number 151254. The company is licensed by the Curaçao Gaming Authority to offer games of chance under license number OGL/2024/1287/0535 in accordance with the National Ordinance on Games of Chance (Landsverordening op de kansspelen, P.B. 2024, no. 157).

Grace Bay B.V. has been granted the approval to operate under the following domains:

1. tipobet365.com
2. tipobet.com

The official certificate for this license was issued on 23rd August 2024.

The company's primary business activities include organizing, marketing, promoting, managing, supporting, and operating all types of remote gaming activities. These encompass a variety of games, betting, and operations related to betting exchanges, interactive casinos, bingos, lotteries, and other interactive games for clients located outside of Curaçao.

Grace Bay B.V. possesses the legal authority to perform all actions necessary to achieve its business objectives in the broadest sense, contributing to its global operational flexibility and growth.

Grace Bay B.V. is committed to upholding the highest standards of Anti-Money Laundering (AML) compliance, adhering to the regulations established by the Curaçao Gaming Authority (CGA) as well as other international regulatory bodies. Operating under the domains tipobet365.com and tipobet.com, the company's AML policy provides a comprehensive framework aimed at identifying, mitigating, and managing risks related to money laundering, terrorist financing, and fraud within its global remote gaming operations.

Grace Bay B.V. conducts a wide range of remote gaming activities, including sports betting, live casinos, poker, slot games, and other interactive games. With the integration of both cryptocurrency and fiat deposits in its operations, this policy outlines specific crypto risk management strategies that apply to both B2C and B2B transactions, ensuring the company's compliance with AML regulations across all jurisdictions in which it operates.

1.2 Objective / Purpose

The primary objectives of this AML policy are to:

- 1) Prevent the use of Grace Bay B.V.'s gaming platforms for money laundering, terrorist financing, proliferation financing or fraudulent activities.
- 2) Ensure compliance with global AML regulations as well as the Curaçao Gaming Authority (CGA) requirements.

- 3) Monitor both fiat and cryptocurrency transactions for any suspicious activity or patterns indicative of illegal behavior.
- 4) Implement robust due diligence processes for customers and business partners, ensuring thorough verification and risk assessment.
- 5) Facilitate the timely reporting of suspicious transactions or activities to the appropriate regulatory or law enforcement authorities.

1.3 Application & Scope

This AML policy is designed to ensure comprehensive compliance with global anti-money laundering standards and applies across all aspects of Grace Bay B.V.'s operations, covering the following:

All Employees, Contractors, and Third-Party Partners: This policy is mandatory for all individuals and entities involved with the company, including full-time staff, part-time employees, contractors, and any third-party service providers or partners. It is the responsibility of these parties to follow AML protocols, undergo required training, and report any suspicious activity in compliance with this policy.

All Transactions on Gaming Platforms: The policy covers all financial transactions, both fiat and cryptocurrency, conducted through Grace Bay B.V.'s gaming platforms (tipobet365.com and tipobet.com). This includes deposits, withdrawals, in-game purchases, and bonus transactions, regardless of the size or frequency of the transactions. Each transaction is subject to monitoring for potential red flags related to money laundering, terrorist financing, proliferation financing or other illicit activities.

All B2C and B2B Operations: The AML policy applies to both business-to-consumer (B2C) and business-to-business (B2B) activities, ensuring compliance across the company's direct consumer operations as well as partnerships, affiliates, and business deals. This includes any risk management protocols associated with customer onboarding, transaction monitoring, and partner due diligence, ensuring that the AML framework is applied consistently across all business relationships.

Global Application Across All Jurisdictions: Although the company operates remotely, this AML policy applies uniformly in all regions where Grace Bay B.V. conducts business. The global nature of the company's services means that AML measures must be adaptable and in line with the specific regulatory requirements and risks posed by the jurisdictions in which it operates.

Cryptocurrency and Fiat Management: Specific risk management procedures for cryptocurrency transactions are included within the policy, alongside traditional fiat currency monitoring. This ensures that both payment methods are equally scrutinized for potential AML risks, with a focus on protecting the platforms from being used for illegal activities.

Due Diligence and Customer Verification: The policy mandates the implementation of Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), and Know Your Customer (KYC) procedures for all users of Grace Bay B.V.'s platforms. This includes identity verification, wallet registration, and ongoing monitoring of player behavior to ensure the platform is not used for illicit purposes.

Reporting of Suspicious Activities: All transactions identified as suspicious or high-risk must be reported to the designated authorities in a timely manner. This includes any unusual account activity, inconsistent transaction patterns, or sudden large deposits or withdrawals that raise concerns. The policy establishes protocols for the escalation and reporting of such activities to the relevant regulatory bodies.

1.4 Review Frequency

Grace Bay B.V. is committed to maintaining an up-to-date and effective Anti-Money Laundering (AML) policy in compliance with the regulations of the Curaçao Gaming Authority (CGA) and global standards, including:

- a) Financial Action Task Force (FATF) recommendations.
- b) European Union 5th Anti-Money Laundering Directive (5AMLD).

- c) USA Patriot Act (for transactions involving USD).

We conduct reviews according to the following schedule:

Annually: The AML policy will be comprehensively reviewed at least once every year to ensure alignment with evolving AML risks, regulatory requirements, and company operations.

Regulatory Changes: An immediate review will be conducted whenever there are significant changes to:

- Curaçao Gaming Authority regulations and guidance.
- Global AML laws, including updates from the Financial Action Task Force (FATF), 5AMLD, and USA Patriot Act, or any other applicable international frameworks.
- Internal changes in the business model, such as expansion into new markets or the introduction of new products or services.

Risk Assessments: Regular reviews will also be conducted if new risks are identified through internal audits, external investigations, or evolving business practices.

The Money Laundering Reporting Officer (MLRO) of Grace Bay B.V. is responsible for conducting these reviews. After each review, any revisions will be submitted to senior management for approval, ensuring that the policy remains compliant with all relevant regulatory standards and effective in addressing the specific AML risks associated with the company's worldwide operations.

1.5 Definitions

Anti-Money Laundering (AML): AML refers to the laws, regulations, and procedures implemented by financial institutions and other regulated entities to detect, prevent, and report money laundering activities. It ensures compliance with both local and global regulations, including the FATF recommendations, 5AMLD, and the USA Patriot Act.

Cryptocurrency (Virtual Assets): Cryptocurrency is a digital or virtual asset that uses cryptography for security and operates on decentralized blockchain technology. It can be used for payments, investments, and transactions, and it presents specific risks related to money laundering, fraud, and terrorist financing due to its pseudonymous nature.

Virtual Asset Service Provider (VASP): A Virtual Asset Service Provider is any individual or entity that facilitates the exchange, transfer, or safekeeping of virtual assets (cryptocurrency), or offers financial services related to the issuance of virtual assets. VASPs must comply with AML regulations, including customer due diligence and reporting requirements.

Know Your Customer (KYC): KYC is a regulatory requirement that obligates companies to verify the identity of their customers and assess the potential risks of illegal activities, including money laundering and terrorist financing. This process includes obtaining personal data, identification documents, and assessing the source of funds.

Customer Due Diligence (CDD): Customer Due Diligence (CDD) refers to the process used to verify the identity of customers, assess the nature of their business relationships, and monitor transactions to prevent money laundering, terrorist financing, and other illicit activities.

Enhanced Due Diligence (EDD): Enhanced Due Diligence (EDD) refers to additional, more rigorous checks and measures taken when dealing with high-risk customers or situations. This includes obtaining more detailed information on the customer's identity, business, and transactions to mitigate potential risks.

Money Laundering: Money laundering is the process of concealing the origin of illegally obtained funds to make them appear legitimate. The process typically involves three stages:

- a) Placement: Introducing illicit funds into the financial system.
- b) Layering: Complex transactions to obscure the origin of the funds.

- c) **Integration:** Reintroducing the funds into the economy as legitimate assets.

Blockchain Analytics: Blockchain analytics is the process of monitoring and analysing blockchain transactions to identify suspicious activity, including the movement of illicit funds, through cryptocurrency networks. It helps detect patterns of money laundering, fraud, and terrorist financing within virtual asset transactions.

Fiat Currency: Fiat currency is any legal tender that is issued by a central authority, such as government-issued currency (e.g., USD, EUR). Transactions involving fiat currency must follow strict AML measures, including monitoring for suspicious activity.

Terrorist Financing: Terrorist financing is the act of providing funds or financial support to individuals, groups, or entities that engage in terrorist activities. This funding may come from both legal and illegal sources and is closely monitored under global AML regulations, including FATF and 5AMLD.

Proliferation Financing (PF): Proliferation financing refers to the act of providing funds or financial services to support the proliferation of weapons of mass destruction (WMD) or related materials. It involves activities that facilitate the development, acquisition, or transfer of nuclear, chemical, or biological weapons, their delivery systems, or related materials, in violation of international treaties and sanctions.

Blockchain Compliance: Blockchain compliance refers to the application of regulatory frameworks (AML, KYC, CFT) to blockchain-based transactions. Companies dealing with cryptocurrency must ensure blockchain compliance by monitoring, auditing, and tracking transactions for suspicious activity.

FATF Travel Rule: The FATF Travel Rule requires VASPs to obtain, hold, and transmit originator and beneficiary information for cryptocurrency transactions above a certain threshold, similar to the requirements for wire transfers in the traditional financial system. This rule helps ensure traceability of cryptocurrency transfers to prevent money laundering and terrorist financing.

5th Anti-Money Laundering Directive (5AMLD): The European Union's 5th Anti-Money Laundering Directive introduces new requirements for cryptocurrency exchanges, wallet providers, and other entities handling virtual assets. It mandates that these entities apply KYC and AML procedures, report suspicious activity, and ensure transparency in cryptocurrency transactions.

USA Patriot Act (Relevant to USD Transactions): The USA Patriot Act requires financial institutions that handle U.S. dollar transactions to implement AML programs, monitor transactions, and report any suspicious activities to FinCEN (Financial Crimes Enforcement Network). This includes virtual asset transactions involving USD.

Illegal Organization: An illegal organization is any entity that engages in activities that are criminalized, such as terrorist groups or organized crime syndicates.

Financing of Illegal Organization: Providing financial support, either directly or indirectly, to an illegal organization or its activities, including its members, with the aim of furthering its unlawful objectives.

Crime: Any act or series of acts that constitute money laundering, terrorism financing, or any related predicate offenses under AML laws and regulations.

Funds: Assets in any form, including physical, digital, tangible, or intangible, such as national currency, foreign currency, virtual currency, property, rights, or any associated profits or income.

Proceeds: Proceeds refer to any funds or assets derived from criminal activity, including any profits or advantages obtained directly or indirectly from illegal acts.

Suspicious Transaction: A transaction is considered suspicious if there are reasonable grounds to believe that it involves the proceeds of crime or is associated with terrorist financing or illegal organizations. This includes both attempted and completed transactions.

Freezing or Seizure: Freezing or seizure is the act of temporarily restricting the movement, transfer, or disposition of funds by an order from a competent authority, pending further investigation.

Beneficial Owner: The individual who ultimately owns or controls a customer or entity, either directly or indirectly. This person benefits from the assets or transactions being conducted on behalf of the entity. Grace Bay B.V. identifies beneficial owners using a 25%+ ownership threshold and verifies their identity through documentation.

Politically Exposed Person (PEP): A Politically Exposed Person (PEP) is someone entrusted with prominent public functions, such as a senior politician, government official, or military leader. The definition also extends to their family members and close associates, as they may pose a higher risk due to their position of influence.

Legal Arrangement: A legal arrangement is a relationship established between two or more parties, typically through contracts or trusts, that does not result in the creation of a distinct legal entity, such as a trust or similar fiduciary arrangement.

Shell Companies: A shell company is a corporation or entity that has no active business operations or significant assets. These companies are often used for legal purposes but can be misused for money laundering, tax evasion, or other illicit activities.

Suspicious Transaction Report (STR): A Suspicious Transaction Report (STR) is a formal report filed by a financial institution or designated entity to relevant authorities when there is suspicion that a transaction may be related to criminal activity, money laundering, or terrorism financing.

Suspicious Activity Report (SAR): A Suspicious Activity Report (SAR) is a formal report submitted to authorities when a financial institution or regulated entity detects a transaction or series of transactions that are suspected to be linked to money laundering, terrorist financing, or other illicit activities. This includes cryptocurrency transactions.

Terrorism Financing: Terrorism financing refers to the provision of funds or financial support to individuals or organizations involved in terrorist activities. Financing can come from legitimate or illicit sources and is aimed at supporting the execution of terrorist acts.

Source of Funds (SOF): The source of funds is the origin of the money used in a transaction. It refers to where the money came from immediately before being used in a particular financial transaction.

Source of Wealth (SOW): Source of Wealth refers to the origin of an individual's overall wealth or assets, which indicates how they have accumulated their financial resources over time.

Sanctions List: A sanctions list is a record of individuals, entities, or countries subject to economic or trade sanctions. Transactions involving individuals or entities on these lists are restricted or prohibited. Grace Bay B.V. must ensure compliance with global sanctions regimes, such as the U.S. Office of Foreign Assets Control (OFAC) and European Union sanctions.

Risk-Based Approach (RBA): A Risk-Based Approach involves assessing and managing risks based on the specific activities of the business. In the context of AML, this means focusing resources on higher-risk customers, transactions, or regions to ensure that the business is not used for money laundering or terrorist financing.

Continuous Transaction Monitoring: Continuous transaction monitoring refers to the ongoing process of reviewing and analysing customer transactions to identify patterns of suspicious activity. For cryptocurrency transactions, this includes identifying rapid movements of funds, structuring of transactions, or interactions with high-risk wallets.

Chain of Ownership: In the context of cryptocurrency, the chain of ownership refers to the history of transfers of a virtual asset, which can be tracked on the blockchain. Monitoring the chain of ownership helps identify whether a cryptocurrency has been used in illicit activities.

Privacy Coins: Privacy coins are cryptocurrencies designed to enhance user anonymity by obscuring transaction details such as sender, receiver, and the amount transferred. Due to their potential misuse in money laundering, privacy coins are subject to increased scrutiny under global AML regulations.

Wallet Providers: Wallet providers are services that offer storage solutions for cryptocurrency. They may be custodial (holding the user's private keys) or non-custodial (where users control their own keys). These providers must implement AML measures, including KYC and transaction monitoring, especially when dealing with large volumes of cryptocurrency.

Counter Terrorism Financing (CTF): Counter Terrorism Financing (CTF) is the set of laws and regulations aimed at detecting and preventing the funding of terrorist organizations. AML policies typically integrate CTF measures to identify and report suspicious.

1.6 AML Regulatory Framework

Grace Bay B.V. adheres to a comprehensive AML regulatory framework to ensure compliance with both local and international standards. This framework encompasses regulations set forth by the Curacao Gaming Authority (CGA) and aligns with global AML standards, including the Financial Action Task Force (FATF) recommendations, the European Union 5th Anti-Money Laundering Directive (5AMLD), the USA Patriot Act (for transactions involving USD), and global cryptocurrency regulations.

1. Curacao Gaming Authority (CGA)

Grace Bay B.V. operates under the regulations set forth by the Curacao Gaming Authority (CGA). The CGA oversees and enforces AML regulations specific to remote gaming and gambling activities. The CGA's requirements include:

AML Policies and Procedures: Implementation of comprehensive AML policies and procedures tailored to the gaming industry.

Customer Due Diligence: Conducting KYC checks and assessing the risk of money laundering for all customers.

Suspicious Activity Reporting: Obligation to report any suspicious activities or transactions to the relevant authorities.

Record-Keeping: Maintaining records of transactions and customer information as required by AML regulations.

2. Financial Action Task Force (FATF) Recommendations

The FATF is recognized as the international standard-setter for AML and counter-terrorism financing (CTF) efforts. Grace Bay B.V. aligns with FATF recommendations, which include:

Risk-Based Approach: Implementing a risk-based approach to identify and mitigate potential AML and CTF risks.

Customer Due Diligence (CDD): Conducting thorough CDD to verify customer identities and assess the risk of money laundering.

Enhanced Due Diligence (EDD): Applying EDD measures for higher-risk customers or transactions.

Suspicious Activity Reporting: Reporting suspicious transactions to the relevant authorities.

Ongoing Monitoring: Continuously monitoring transactions and customer activities for signs of suspicious behavior.

3. European Union 5th Anti-Money Laundering Directive (5AMLD)

The 5AMLD is a key regulatory framework in the European Union that addresses AML and CTF requirements for cryptocurrency entities. Grace Bay B.V. complies with the following aspects of 5AMLD:

Customer Identification: Mandatory KYC procedures for cryptocurrency exchanges and wallet providers.

Transaction Reporting: Requirements to report suspicious transactions and maintain transparency in cryptocurrency transactions.

Enhanced AML Controls: Implementation of robust AML controls and procedures for virtual asset service providers (VASPs).

Cross-Border Cooperation: Ensuring cooperation with other EU member states in the fight against money laundering and financing.

4. USA Patriot Act (for Transactions Involving USD)

The USA Patriot Act requires financial institutions handling U.S. dollar transactions to adhere to specific AML

regulations. Grace Bay B.V. complies with the following provisions:

AML Programs: Implementation of AML programs to monitor and report suspicious activities involving USD transactions.

Transaction Monitoring: Continuous monitoring of transactions for signs of money laundering and terrorist financing.

Reporting Obligations: Reporting suspicious transactions to the Financial Crimes Enforcement Network (FinCEN) and other relevant authorities.

5. Cryptocurrency Regulations Worldwide

Grace Bay B.V. ensures compliance with global cryptocurrency regulations to address the unique risks associated with virtual assets. Key aspects include:

Regulatory Compliance: Adhering to regulations set by relevant authorities in jurisdictions where cryptocurrency transactions occur.

AML Measures for VASPs: Implementing AML measures for virtual asset service providers, including KYC and transaction monitoring.

Global Sanctions Compliance: Ensuring compliance with international sanctions regimes and restrictions related to cryptocurrency transactions.

Blockchain Analytics: Utilizing blockchain analytics tools to monitor and investigate cryptocurrency transactions for potential illicit activities.

Grace Bay B.V. adheres to the National Ordinance on the Reporting of Unusual Transactions (NORUT), the National Ordinance Identification when Rendering Services (NOIS), and the Sanctions National Ordinance. The company follows local sanctions mechanisms, including mandatory adherence to all sanction decrees published by the CGA, and FIU sanctions-triggered reporting. Any sanctions match triggers a UTR/STR to the FIU via goAML.

In compliance with these regulatory frameworks, Grace Bay B.V. upholds AML and CTF standards to foster a secure and transparent environment for its remote gaming activities and cryptocurrency transactions.

1.7 Governance of AML/CFT/PF Program

The AML/CFT/PF program is approved by the Board of Grace Bay B.V. and includes periodic testing through internal audits to ensure effectiveness. The program links the Business Risk Assessment (BRA), Customer Acceptance Policy (CAP), Customer Risk Assessment (CRA), and Customer Due Diligence (CDD) to form a cohesive compliance framework. The Board reviews the program annually or upon significant changes.

2. Risk Based Approach



2. Risk Based Approach

The Risk-Based Approach (RBA) for Grace Bay B.V. is designed to meet the regulatory requirements of the Curacao Gaming Authority (CGA) and align with global AML standards, such as the FATF recommendations, European Union Directives, and various international regulatory frameworks. Grace Bay operates globally, and the RBA is essential in managing the risks associated with money laundering, terrorist financing, and cryptocurrency usage in its remote gaming activities.

Board-approved BRA Methodology: The Business Risk Assessment (BRA) methodology is approved by the Board of Grace Bay B.V. It is conducted annually or upon significant changes in business operations. Data sources include internal transaction data, customer profiles, external reports from FATF, and blockchain analytics.

Risk ranking logic: Risks are ranked using a matrix of likelihood and impact, as detailed in 2.2, with scores leading to low, medium, high, or very high risk levels.

Risk appetite: Grace Bay B.V. has a low risk appetite for AML/CFT/PF risks, meaning it will not accept high-risk customers or transactions that cannot be mitigated to an acceptable level. Decline thresholds are set for high-risk profiles where risks exceed acceptable levels after mitigation.

The risk assessment covers all four risk domains as required: customer, geography, products/services, and distribution channels.

Expand CRA and CAP: Customer Risk Assessment (CRA) uses risk indicators such as geography, transaction patterns, source of funds. Customer Acceptance Policy (CAP) includes acceptance criteria (e.g., full KYC completion, low-risk profile), and decline thresholds (e.g., high-risk jurisdiction without mitigation, failure to provide documents).

2.1.1. Type of Customers and Their Activities

Grace Bay B.V. primarily serves customers aged 25-32, mostly men, with a global reach. The company does not target high-net-worth individuals, and deposits and withdrawals are subject to daily limits to prevent money laundering and suspicious activity. Key considerations regarding customer risk include:

Gaming Behavior: High-risk activities are flagged, such as large deposits following small ones or erratic gameplay patterns.

High-Risk Customers: Customers drawn to gaming bonuses, such as the 100% first deposit bonus, could indicate higher risk for potential abuse.

KYC Procedures: Full Know Your Customer (KYC) verification, including identity checks for both bank and crypto transactions, is required to prevent fraudulent activities. For crypto transactions, wallet address registration is mandatory, preventing the use of unverified wallets.

2.1.2. The Countries or Geographic Areas in Which the Company Does Business

Grace Bay B.V. operates globally, but certain jurisdictions pose higher risks due to varying regulatory standards. The company uses FATF recommendations and other regulatory frameworks to assess geographical risk:

High-Risk Jurisdictions: Countries listed as high-risk by FATF or those with weak AML regulations are either avoided or subject to enhanced due diligence (EDD).

Moderate-Risk Jurisdictions: Countries requiring more stringent monitoring due to their inclusion on the FATF grey list or other international watchlists, leading to additional customer scrutiny and transaction limits.

Global Compliance: The company maintains a global compliance standard, monitoring jurisdictions for regulatory changes to ensure ongoing alignment with international AML and counter-terrorism financing (CTF) obligations.

2.1.3. Customer Risk Assessment

Grace Bay B.V. performs comprehensive customer risk assessments to identify and manage potential AML risks posed by clients globally. Key factors include:

Geographical Risk: Grace Bay operates in multiple jurisdictions, requiring special attention to customers from higher-risk countries identified by the FATF or other international bodies. Enhanced due diligence (EDD) is applied to customers from high-risk or sanctioned jurisdictions to ensure compliance with global AML laws.

Customer Demographics: The company serves customers predominantly in the 25-32 age range, mostly men. While this demographic may not inherently suggest elevated AML risks, additional scrutiny is applied to customers exhibiting high-value or irregular deposit and withdrawal patterns.

Customer Behavior Monitoring: Transaction monitoring systems flag suspicious behavior, such as rapid changes in deposit sizes or unusual gaming behavior. Procedures include:

- Verifying bank account details and matching them with customer data.
- Ensuring wallet addresses for cryptocurrency deposits are registered and verified before use.
- Monitoring transaction history for abnormal spikes in deposit amounts or unusual gaming activity.

2.1.4. Transaction Risk Management

Transaction risk is managed through robust monitoring and KYC procedures, focusing on high-value transactions, cryptocurrency usage, and patterns indicative of suspicious activity.

High-Value Transactions: Transactions exceeding predefined daily limits or unusual in size relative to a customer's historical activity are flagged for further investigation.

Cryptocurrency Transactions: Due to the inherent risks of anonymity in cryptocurrency:

- Only widely recognized cryptocurrencies (such as Bitcoin and Ethereum) are accepted, ensuring higher transparency and traceability.
- Cryptocurrency-to-fiat conversions follow strict KYC and EDD protocols, with sudden or large transactions subject to detailed scrutiny.
- Blockchain analysis tools are used to track crypto activity and ensure compliance with AML regulations.

2.1.5. Services Risk (Product & Service Risk Factors)

Given the nature of its remote gaming activities, Grace Bay B.V. encounters inherent risks related to the services offered:

Gaming Bonuses: Promotions such as deposit bonuses can attract fraudsters or high-risk players seeking to exploit the system. The company closely monitors bonus activity for patterns of abuse, including suspicious transfers and bonus withdrawals.

In-Game Purchases and Bets: Unusual bet patterns, including excessive wins or losses and transfers between player accounts, are scrutinized to detect possible money laundering schemes through layering techniques.

Cryptocurrency Transactions: The use of cryptocurrencies, while offering privacy, increases the risk of anonymity and financial crime. Grace Bay mitigates this by accepting only a limited set of widely accepted cryptocurrencies (e.g., Bitcoin, Ethereum) and employing blockchain analysis tools.

2.1.6. Geographical Risk and Jurisdictional Exposure

Grace Bay's global operations expose it to varying levels of AML risk, necessitating a tiered risk assessment approach based on the FATF and other global lists:

High-Risk Jurisdictions: Transactions involving customers from countries on FATF's high-risk, or sanctioned lists are prohibited.

Moderate-Risk Jurisdictions: Customers from jurisdictions flagged as moderate risk are subject to enhanced due diligence measures, including stricter transaction monitoring and reporting protocols.

2.1.7. Cryptocurrency Risk Management

Cryptocurrencies introduce additional risks in online gaming operations. Grace Bay's approach to managing these risks includes:

Accepted Cryptocurrencies: The company limits the use of cryptocurrencies to those that are highly liquid and compliant with global AML standards, reducing exposure to privacy-focused or obscure tokens.

KYC for Crypto Transactions: Grace Bay ensures that all customers undergo comprehensive KYC procedures before engaging in cryptocurrency transactions, including the verification of wallet addresses.

Blockchain Monitoring: Tools like Chainalysis are used to track cryptocurrency transactions and identify suspicious patterns, ensuring that funds are not linked to illicit activities or sanctioned entities.

2.1.8. Delivery Channel Risk

The delivery channels used for both B2C and B2B gaming activities present unique risks, particularly for crypto transactions:

Bank Transactions: KYC checks are applied for all deposits and withdrawals via traditional banking channels. Only matching player names and bank account holders are accepted.

Crypto Transactions: Cryptocurrency channels are riskier due to the potential for anonymous transactions. The company mitigates this by requiring customers to register and pre-approve their wallet addresses. Any attempt to change wallets is blocked, and blockchain analysis is applied to detect suspicious activities.

2.1.9. Technological Development Risk Assessment

Grace Bay B.V. assesses risks from new technologies and delivery channels, such as AI in transaction monitoring or new crypto protocols, to ensure they do not increase AML risks (as per Reg. II.3). Annual reviews of delivery channels like mobile and web apps are conducted to identify vulnerabilities.

2.1.10. Third-Party Risk

Grace Bay relies on third-party service providers for payments and blockchain analytics, and these partners are carefully vetted to ensure they comply with AML standards:

Payment Service Providers: Banks and financial institutions involved in transactions are subject to rigorous due diligence to ensure they adhere to global AML regulations.

Blockchain Analytics Providers: Service providers used for cryptocurrency analysis must demonstrate compliance with international AML and CTF regulations.

2.1.11. Ongoing Monitoring and Reporting

Grace Bay has implemented a robust, real-time monitoring system to detect suspicious transactions:

Suspicious Activity Reporting (SAR): All flagged transactions are reported to the appropriate regulatory bodies in Curacao or relevant international authorities.

Ongoing Due Diligence: Customer profiles are updated regularly, and high-risk customers are subject to additional reviews and monitoring to detect any changes in risk levels.

Periodic Review of Policies: The AML policy, including the RBA, is regularly reviewed and updated to ensure ongoing compliance with global regulatory changes.

2.1.12. Commitment to Managing Transaction Risks

The company is committed to mitigating transaction risks associated with its global gaming operations:

Transaction Limits: Daily deposit and withdrawal limits help to minimize the risk of large-scale money laundering activities.

Blockchain Monitoring: For crypto transactions, Grace Bay employs blockchain analysis tools to monitor the origin of funds, identifying potentially illicit activities such as links to sanctioned entities or suspicious wallet behaviors.

Ongoing Transaction Reviews: Transactions are reviewed in real-time to detect unusual patterns or behaviors. High-risk transactions undergo enhanced scrutiny, ensuring compliance with global AML and CTF regulations.

2.1.13. Mitigation Measures

Grace Bay B.V. has implemented several layers of mitigation measures to address the various risks inherent in its operations:

Enhanced Due Diligence (EDD): For customers from high-risk jurisdictions or those conducting high-value transactions, EDD measures are in place, including in-depth identity verification and increased transaction monitoring.

Transaction Monitoring: Real-time monitoring systems detect suspicious transactions, including significant deviations from normal transaction patterns, high-volume crypto-to-fiat conversions, and irregular deposit/withdrawal activities.

Regular Risk Assessments: The company conducts regular risk assessments to evaluate its risk profile and adjust its AML policies to reflect changes in its customer base, product offerings, or the regulatory landscape.

Staff Training: Employees undergo periodic AML/CTF training, focusing on identifying red flags, suspicious behavior, and reporting requirements. Staff are also trained on crypto-specific risks, including wallet verification and blockchain monitoring.

Regulatory Compliance: Regular internal audits ensure that the company's AML measures comply with Curacao's Gaming Control Board requirements and international standards.

2.1.14. Commitment to Security and Compliance

Grace Bay B.V. is committed to maintaining the highest standards of security and compliance across its operations:

Data Security: Customer data is securely stored, encrypted, and handled following GDPR and other global data protection laws.

Compliance with AML Regulations: The company adheres to the AML regulations of the Curacao Gaming Authority and continuously updates its policies to align with international AML/CTF guidelines.

2.1.15. Commitment to Secure Delivery Channels

Grace Bay B.V. is dedicated to ensuring the secure use of all delivery channels:

Pre-Approved Wallets: For crypto transactions, customers can only use pre-approved wallets, ensuring traceability of funds and preventing fraud.

Compliance with Global Crypto Regulations: The company monitors global crypto regulations and adjusts its processes to comply with AML and KYC rules in all jurisdictions where it operates.

Adhering to this detailed Risk-Based Approach enables Grace Bay B.V. to ensure that its remote gaming operations comply with both Curacao Gaming Authority regulations and international AML/CTF standards. This approach fosters a secure and transparent environment, minimizing the risk of money laundering, terrorist financing, and other financial crimes.

2.2. Risk Matrix for Likelihood and Impact

Risk Matrix for Likelihood and Impact as following the risk assessment approach provided. It integrates global AML regulations, Curacao Gaming Authority requirements, and the company's business activities.

2.2.1. Risk Matrix for Likelihood and Impact for Grace Bay B.V.

Impact \ Likelihood	No Likelihood	Very Low Likelihood	Low Likelihood	Moderate Likelihood	High Likelihood	Very High Likelihood
No Impact	0	0	0	0	1	1
Very Low Impact	0	1	2	2	3	3
Low Impact	0	2	3	3	4	4
Moderate Impact	0	2	3	4	5	5
High Impact	1	3	4	5	5	5
Very High Impact	1	3	5	5	5	5

2.2.2. Likelihood Assessment for Grace Bay B.V.

0: No Likelihood – The risk is not expected to occur, e.g., customers depositing through illegal channels when strict wallet verification and KYC are in place.

1: Very Low Likelihood – Minimal chance of occurrence, e.g., a minor regulatory change with negligible impact on operations.

2: Low Likelihood – Unlikely but possible, e.g., minor discrepancies in customer identity during onboarding.

3: Moderate Likelihood – Possible, but not frequent, e.g., instances of minor fraud or unusual customer behavior.

4: High Likelihood – A significant chance of occurrence, e.g., risky customer profiles with higher levels of suspicious activities.

5: Very High Likelihood – The event is expected, e.g., regions with high AML risk factors, frequent changes in regulation.

2.2.3. Impact Assessment for Grace Bay B.V.

0: No Impact – No effect on business operations, e.g., internal minor issues with no external exposure.

1: Very Low Impact – Negligible impact on operations, e.g., minor KYC issues resolved without escalation.

2: Low Impact – Limited operational or reputational impact, e.g., minor transaction delays due to verification.

3: Moderate Impact – Noticeable impact on operations, e.g., suspicious activity that requires manual investigation but does not breach regulations.

4: High Impact – Significant operational or reputational damage, e.g., a failure in AML controls leading to flagged transactions.

5: Very High Impact – Severe impact on operations or reputation, e.g., involvement in a major money laundering scandal or regulatory penalties.

2.2.4. Risk Matrix Application for Grace Bay B.V.

- 1) **Customer Risk (Moderate Likelihood, High Impact):** Customers aged 25-32, largely men, may engage in high-risk behavior due to bonuses and gambling habits, requiring enhanced due diligence.
- 2) **Geographical Risk (Low Likelihood, High Impact):** Operating worldwide, including countries with strict AML controls, means there's a low likelihood but potentially high impact from compliance breaches.
- 3) **Transaction Risk (Moderate Likelihood, Moderate Impact):** 2000-4000 transactions daily, mostly crypto and bank, carries moderate likelihood but requires strict monitoring to avoid fraud.
- 4) **Service Risk (High Likelihood, Moderate Impact):** Offering high-risk services like live casino and poker, which can attract illicit activities, demands enhanced due diligence and monitoring.

2.3. Risk Categories and Factors

The detailed breakdown of Risk Categories and Factors for Grace Bay B.V. addresses the various AML/CFT risks across customer, geographical, product, transaction, and compliance-related factors. The risk-based approach should help the company implement robust AML measures aligned with the nature of its global business and the requirements of the Curacao Gaming Control Board.

2.3.1. Customer Risk

Factors:

- **Customer Profile:** Primarily men aged 25-32, potentially tech-savvy, engaging in gambling activities.
- **Transaction Patterns:** Sudden increases in deposit amounts or irregular transactions.
- **High-Risk Customer Segments:** Customers who regularly use bonuses or special promotions, particularly high bonus offers (e.g., 100% first deposit bonus), can attract fraudsters.
- **Inconsistent Payment Details:** Mismatched names between customer accounts and deposit sources, especially for bank transfers.
- **Geographical Considerations:** Customers from countries with weak AML/CFT regulations or on FATF high-risk jurisdictions.

Risks:

- Potential use of gaming platforms for laundering illicit funds through rapid deposit and withdrawal

cycles.

- High-risk jurisdictions increasing exposure to potential sanctions or penalties.
- Fraudulent activities involving promotions and bonus misuse.

2.3.2. Geographical Risk

Factors:

- **Operation in High-Risk Jurisdictions:** Operating worldwide, including countries with high AML/CFT risks.
- **Regulatory Environment:** Compliance with differing AML/CFT regulations across multiple jurisdictions.
- **Country-Specific Risk:** Risks associated with countries that have weaker AML regulations or high levels of organized crime.
- **FATF Grey/Blacklist Countries:** Countries under increased monitoring or non-compliant with FATF standards.

Risks:

- Operating in high-risk jurisdictions can increase the exposure to money laundering, terrorist financing, and other criminal activities.
- Potential penalties or fines due to non-compliance with country-specific regulations.

2.3.3. Transaction Risk

Factors:

- **Volume and Frequency:** 2,000-4,000 daily transactions, with a volume between \$50,000 - \$100,000, largely crypto and bank deposits.
- **Nature of Transactions:** Use of cryptocurrencies for both deposits and withdrawals present unique challenges related to traceability.
- **Unusual or Large Transactions:** Significant deviations in deposit sizes or patterns, such as a sudden increase in the size or frequency of transactions.
- **Cross-Border Transfers:** Large sums transferred internationally or between accounts that may not align with customer profiles.

Risks:

- Crypto transactions can be used to obscure the origin of funds, presenting a higher risk of money laundering.
- Frequent cross-border transactions, especially with crypto, increase exposure to regulatory scrutiny.

2.3.4. Product and Service Risk

Factors:

- **Remote Gaming Services:** High-risk products such as interactive casinos, live casino, sports betting, poker, slots, and crash games.
- **Promotional Offers:** High-value bonuses, such as 100% first deposit bonus, which can attract both high-

risk customers and fraudsters.

- **In-Game Purchases:** Players making frequent or large in-game purchases, potentially with laundered funds.
- **Multiple Deposit Methods:** Offering both bank transfers and cryptocurrency deposit options can create vulnerabilities if not closely monitored.

Risks:

- Casino and betting activities are frequently targeted by criminals to launder funds, using gaming platforms to deposit, withdraw, and move funds.
- Promotional offers may inadvertently attract customers looking to exploit bonuses for illicit gain.

2.3.5. Crypto-Specific Risk

Factors:

- **Accepted Cryptocurrencies:** Variety of cryptocurrencies accepted for transactions.
- **Wallet Address Registration:** Customers must register their wallet address for deposits and withdrawals, and the address cannot be changed afterward.
- **Volatility and Anonymity:** The volatile nature of cryptocurrency and the anonymity it provides can make monitoring difficult.
- **Conversion to FIAT:** Regular conversion of crypto to fiat currency may pose challenges in tracking the source and legitimacy of the funds.

Risks:

- High levels of anonymity in crypto transactions can facilitate the movement of illicit funds without detection.
- Failure to monitor crypto deposits and withdrawals adequately could result in funds being laundered through Grace Bay's platforms.

2.3.6. Payment Method Risk

Factors:

- **Bank Transfers:** Transfers where the name on the bank account differs from the player's name could indicate money laundering or account misuse.
- **Crypto Transactions:** Increased risk of money laundering through rapid crypto deposits and withdrawals without strong KYC/AML controls.
- **Payment Instrument Controls:** Registration of crypto wallets and verification of bank accounts help to mitigate some risks but need to be rigorously enforced.

Risks:

- Misuse of bank transfers and crypto wallets could indicate attempts to launder money through Grace Bay's platforms.
- Complexities in monitoring transactions across both bank and crypto may expose the platform to regulatory risks.

2.3.7. Behavior Risk

Factors:

- **Gambling Behavior:** Unusual gambling patterns, such as frequent large bets or a sudden spike in activity.
- **Fraudulent Behavior:** Use of multiple accounts to exploit bonuses, manipulate game outcomes, or transfer funds across accounts.
- **Irregular Withdrawals:** Players making large withdrawals without proportional gaming activity.

Risks:

- Fraudulent behavior can increase exposure to financial losses and regulatory penalties.
- Exploiting gaming systems, such as moving funds between accounts via bonus abuse or suspicious withdrawals, is a common laundering tactic.

2.3.8. Compliance Risk

Factors:

- **Differing Regulatory Standards:** Operating in multiple jurisdictions with various AML requirements, requiring compliance with local and international regulations.
- **FATF Compliance:** Ensuring that the company adheres to the latest FATF recommendations and updates, particularly regarding cryptocurrency.
- **Regulatory Scrutiny:** Potential for audits or investigations from multiple regulators, particularly in high-risk regions.

Risks:

- Failing to comply with global AML/CFT standards could result in fines, penalties, or loss of licenses.
- Regulatory scrutiny may increase as a result of operating in jurisdictions with stricter compliance requirements.

2.3.9. Reputational Risk

Factors:

- **Public Perception:** Association with money laundering activities or fraudulent behavior can severely damage the company's reputation.
- **Regulatory Penalties:** Fines or sanctions from regulators could damage the company's image and relationships with banking and payment partners.
- **Negative Media Coverage:** Media reports about the company's involvement in money laundering or fraud could result in loss of customer trust.

Risks:

- Loss of customer trust and market share if the company is linked to financial crimes.
- Potential negative press, impacting partnerships, and business expansion.

2.3.10. Operational Risk

Factors:

- **System Failures:** Technical issues in tracking, monitoring, or reporting transactions, particularly with crypto and in-game purchases.
- **AML Systems and Controls:** Weaknesses in automated transaction monitoring systems or failure to update AML procedures as the business expands.
- **Employee Competency:** Ensuring employees handling KYC and AML processes are adequately trained and remain vigilant against suspicious activity.

Risks:

- Weak AML systems and operational inefficiencies may result in missed detection of illicit activities.
- Failure to update procedures or systems may expose the company to regulatory fines or operational disruptions.

2.3.11. Political and Legal Risk

Factors:

- **Changing Regulations:** Cryptocurrency regulations, gaming laws, and AML requirements may change quickly in various jurisdictions.
- **Political Instability:** Operating in countries with unstable political environments may increase regulatory and legal risks.
- **Sanctions:** Risk of dealing with customers or businesses under international sanctions.

Risks:

- Rapidly changing regulations could impact the ability to operate smoothly and in compliance with local laws.
- Sanctions violations could result in severe legal penalties.

2.3.12. Delivery/Distribution Channel Risk

Factors:

- Online platforms, mobile apps, API integrations for B2B operations.

Risks:

- Vulnerabilities to cyber attacks, unauthorized access, or misuse for illicit transactions.

2.4. Detailed Risk Matrix for Grace Bay B.V

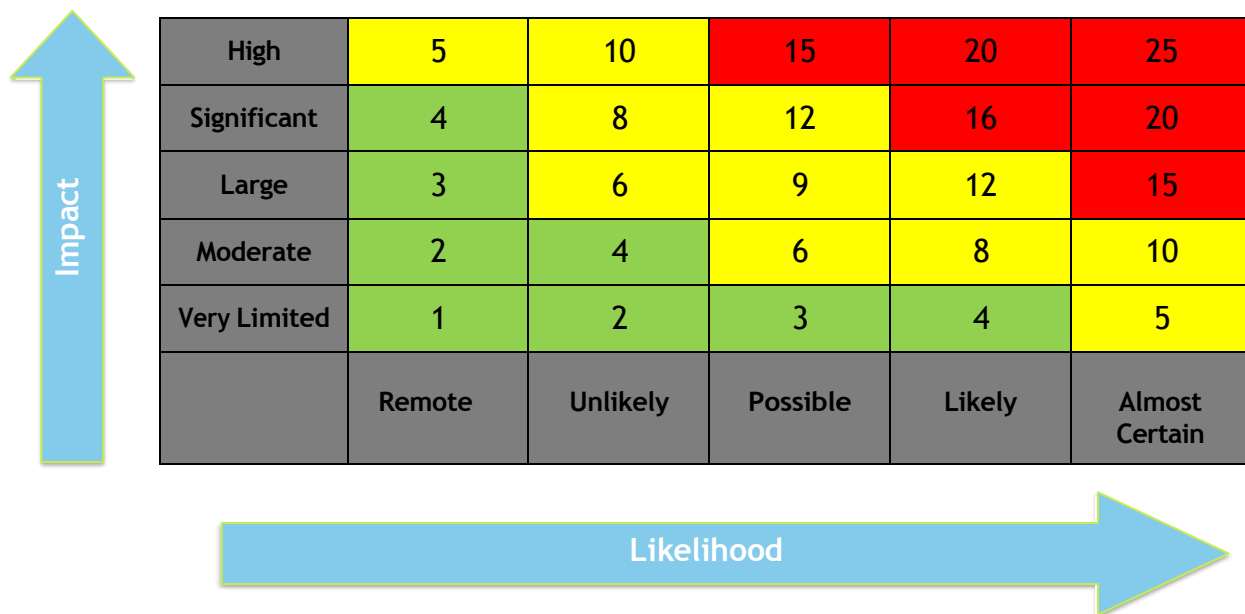
The Likelihood Score is rated from 1 (Very Low) to 5 (Very High), and the Impact Score is rated from 1 (Minimal Impact) to 5 (Severe Impact).

The Risk Level is determined by multiplying the Likelihood by the Impact and categorizing it as Low (1-5), Medium (6-10), High (11-15), Very High (16-25).

Risk Factor	Likelihood Score (1-5)	Impact Score (1-5)	Risk Level
Customer Profile	4	4	16 (Very High)
Transaction Patterns	3	4	12 (High)
High-Risk Customer Segments	4	3	12 (High)
Inconsistent Payment Details	4	5	20 (Very High)

Geographical Risk (High-Risk Jurisdictions)	5	4	20 (Very High)
FATF Grey/Blacklist Countries	3	5	15 (High)
Unusual/Large Crypto Transactions	5	4	20 (Very High)
Cross-Border Transfers	4	3	12 (High)
Remote Gaming Activities	4	4	16 (Very High)
High-Value Bonuses	3	4	12 (High)
In-Game Purchases	3	3	9 (Medium)
Multiple Payment Methods (Crypto + Bank)	5	4	20 (Very High)
Crypto Wallet Anonymity	4	5	20 (Very High)
Customer Wallet Registration	3	3	9 (Medium)
Crypto-Fiat Conversion	4	4	16 (Very High)
Sudden Gambling Pattern Changes	3	4	12 (High)
Fraudulent Account Activity	4	5	20 (Very High)
Inconsistent Withdrawals	4	4	16 (Very High)
Differing Regulatory Standards (Jurisdictions)	5	4	20 (Very High)
Regulatory Scrutiny	3	5	15 (High)
Reputational Damage (Fraud/Money Laundering)	3	5	15 (High)
Negative Media Coverage	3	4	12 (High)
AML Systems Failure	3	5	15 (High)
Systemic Technical Issues	3	4	12 (High)
Employee Competency in AML	3	4	12 (High)
Changing Regulations	4	4	16 (Very High)
Political Instability in Regions	2	4	8 (Medium)
International Sanctions Risk	3	5	15 (High)

The above risk ratings depend on the impact and likelihood matrix given below:



The diagram illustrates the Impact and Likelihood matrix. A vertical blue arrow on the left points upwards and is labeled 'Impact'. A horizontal blue arrow at the bottom points to the right and is labeled 'Likelihood'. The matrix itself is a 6x6 grid where the rows represent Impact levels and the columns represent Likelihood levels. Each cell contains a numerical risk rating. The colors of the cells indicate the risk level: red for Very High Risk (ratings 16-25), yellow for High Risk (ratings 11-15), and green for Medium Risk (ratings 6-10).

High	5	10	15	20	25
Significant	4	8	12	16	20
Large	3	6	9	12	15
Moderate	2	4	6	8	10
Very Limited	1	2	3	4	5
	Remote	Unlikely	Possible	Likely	Almost Certain

2.4.1 Risk Level Summary:

1. Very High Risk (16-25): Immediate focus needed on these factors due to their potential to severely impact the business. Key areas include crypto-related risks, geographical risks, customer profiles, and inconsistencies in payment methods.
2. High Risk (11-15): Requires strong monitoring and mitigation, especially around customer behavior, regulatory compliance, and reputational risks.
3. Medium Risk (6-10): Risks that require ongoing management but have lower immediate impact, including political instability and employee competency.



3-Customer Due Diligence

3. Customer Due Diligence (CDD)

The Customer Due Diligence (CDD) outlines the procedures and requirements for Grace Bay B.V. in relation to anti-money laundering (AML) and countering the financing of terrorism (CFT). The CDD is in line with the regulations of the Curacao Gaming Control Board, applicable global AML regulations, and the specific nature of business activities of Grace Bay B.V., which involves remote gaming, online betting, casinos, and cryptocurrency transactions.

3.1. CDD Objectives

The primary objectives of CDD are to:

- Verify the identity of customers.
- Understand the nature of the customer's activities and the source of funds.
- Mitigate risks associated with money laundering, terrorist financing, and other illicit activities.
- Comply with regulatory requirements from the Curacao Gaming Authority and international AML standards.

3.2. When CDD is Required

Grace Bay B.V. shall conduct CDD in the following circumstances:

- **New Customer Onboarding:** Before establishing a business relationship with any customer.
- **Significant Transactions:** For transactions involving \$10,000 or more, including cryptocurrency conversions to fiat currency.
- **Suspicious Activity:** When suspicious transactions or activities are identified.
- **Changes in Customer Behavior:** Sudden changes in customer behavior or high-volume transactions outside the norm (e.g., large crypto deposits).
- **Periodic Reviews:** Regular CDD checks on existing customers, particularly high-risk ones.

CDD is required when a customer's cumulative daily deposits or wagers reach NAFL 4,000 (as per Reg. III.1, III.3). Calculation is based on the sum of all transactions in a 24-hour period. Customers may play games but cannot make deposits or withdrawals until CDD is completed once the threshold is reached (CDD timing rules).

CDD for existing customers: Existing customers are subject to periodic CDD reviews, especially if risk profiles change or upon regulatory request.

3.3. CDD Procedures

Grace Bay B.V. shall implement a thorough CDD process for both B2C and B2B operations, including:

3.3.1. Identification and Verification

Individual Customers:

- a) Collect and verify the customer's full name, date of birth, residential address, nationality, place of birth, and identification documents (passport, driver's license, or national ID).
- b) Verify the customer's identity using reliable third-party verification systems and databases.
- c) For cryptocurrency transactions, require customers to provide a verified wallet address before making any deposits or withdrawals. The wallet address must remain unchanged during the relationship.

Corporate Clients (B2B):

- a) Obtain and verify the legal entity's full name, registration number, legal structure, and the address of the registered office.
- b) Identify the beneficial owners (anyone with a 25% or more interest in the entity) and verify their identity.
- c) Review the company's activities, including the nature of its business and the source of funds.

For beneficial owners (BO):

- Identify BOs with 25%+ ownership threshold, verify their identity using the same procedures as individual customers.

Sanctions screening integration in CDD:

- During CDD, customers are screened against UN/EU/local sanctions lists and for PF risks. If a match is found, assets are frozen, and the matter is reported.

3.3.2. Customer Risk Profiling

Grace Bay B.V. shall categorize customers into low, medium, and high-risk profiles based on several factors:

- a) Geographical Risk: Customers from FATF high-risk jurisdictions, such as countries on the FATF's grey are considered high-risk.

- b) Transaction Patterns: Sudden large deposits, frequent cryptocurrency transactions, or withdrawals exceeding thresholds will be flagged for further scrutiny.
- c) Source of Funds: Determine whether the customer's source of funds (crypto or fiat) is legitimate and consistent with their profile.
- d) Bonuses & Promotions: Customers attracted by large bonuses, such as the 100% first deposit bonus, may pose a higher risk and should be monitored more closely.

3.3.3. Ongoing Monitoring

Grace Bay B.V. will implement ongoing monitoring for all customers, focusing on:

- 1) Transaction Monitoring: Regularly review transaction patterns and the customer's deposit and withdrawal behavior.
- 2) Gaming Behavior Monitoring: Cross-check game logs to detect anomalies, such as bonus transfers to different accounts, potential fraud, or abuse of the gaming system.
- 3) Cryptocurrency Monitoring: Use advanced blockchain analysis tools to track the source and destination of cryptocurrency transactions. For example, monitoring tools should detect links to illicit or blacklisted wallet addresses using tools like Chainalysis or similar platforms.

3.4. Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) is required for customers posing a higher risk of money laundering or terrorist financing. High-risk customers include:

- a) Politically Exposed Persons (PEPs): Identifying and assessing any customers with political influence or who hold a public office.
- b) High-Risk Jurisdictions: Customers from countries with high levels of corruption or inadequate AML controls.
- c) Large or Unexplained Crypto Transactions: Customers engaging in significant cryptocurrency activities that are inconsistent with their profile.

In these cases, Grace Bay B.V. will:

- a) Collect additional identification documents.
- b) Request proof of source of funds.
- c) Closely monitor all transactions, with enhanced scrutiny on large deposits or suspicious activities.
- d) Require senior management approval for maintaining business relationships with high-risk customers.

3.5. Simplified Due Diligence (SDD)

In cases where customers pose a low risk (e.g., customers from countries with strong AML frameworks or those making small transactions below risk thresholds), Simplified Due Diligence (SDD) may be applied. SDD involves:

- a) Less frequent verification updates.
- b) Reduced documentation requirements.
- c) Basic monitoring based on the low-risk profile of the customer.

3.6 Failure to Conduct Customer Due Diligence

Failure to properly conduct CDD exposes Grace Bay B.V. to significant risks, including:

Regulatory Penalties: Non-compliance with the Curacao Gaming Control Board's requirements and global AML regulations may lead to fines, suspension, or revocation of licenses.

Reputational Risk: Inadequate CDD can damage the company's reputation and lead to the loss of trust from both customers and regulators.

Criminal Liability: Engaging with customers involved in money laundering, terrorist financing, or other illicit activities can lead to legal consequences, including criminal prosecution of company officers.

Financial Losses: Allowing customers to exploit the platform for illegal purposes can result in financial losses due to fines, frozen assets, or customer attrition.

Termination rules: If required documents are not obtained within 30 days, the account will be terminated (as per Reg. III.3 and III.8).

3.7. Suspicious Activity Reporting (SAR)

All staff involved in customer transactions are trained to detect and report suspicious activities and unusual transactions in accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT) and Reg. IV.1 of the AML/CFT/CFP Regulations. Unusual transactions (UTRs) must be reported to the Financial Intelligence Unit (FIU) Curaçao via goAML without delay. If the FIU or MLRO determines the transaction is suspicious after analysis, it becomes a Suspicious Transaction Report (STR) or SAR. Reports may be submitted in bulk for multiple related incidents, following FIU documentation rules (e.g., including all transaction details, supporting documents, and rationale).

Suspicious or unusual activities are identified based on objective (fact-based) and subjective (judgment-based) indicators. All staff must be trained to recognize these, and any flagged activity must be escalated to the MLRO for review. If a UTR is not submitted to the FIU, internal logs documenting the decision (with reasons and signatures) must be maintained for at least 5 years.

It is strictly prohibited to tip off customers or third parties about investigations, reports, or suspicions (e.g., no disclosure that a transaction has been flagged or reported). Sanctions-triggered UTRs (e.g., matches on UN/EU/local lists) must be reported immediately to the FIU via goAML.

Objective Indicators (Mandatory Triggers - Automatic Reporting Required):

These are fact-based circumstances that deem a transaction unusual per the Decree Indicators Unusual Transactions (PB 2015, no. 73, Annex F):

- Transactions reported to the Police, Department of Justice, or other authorities in connection with money laundering (ML), terrorist financing (TF), or proliferation financing (PF).
- Transactions by or on behalf of a natural or legal person, group, or entity named on a sanctions list under the Sanctions National Ordinance (N.G. 2014, no. 55), including UN, EU, or local lists published by the CGA.
- Transactions of NAf. 5,000 or more (or equivalent in any currency), regardless of payment form (cash, check, electronic, non-physical, or cashless), including:
 - o Cashless transactions of NAf. 5,000 or more (e.g., transfers from the casino's bank account to a local or international account at the client's request).
 - o Accepting or releasing deposits of NAf. 5,000 or more at the client's request.
 - o Sale of chips, tokens, or credits to a customer of NAf. 5,000 or more.
 - o Cash-outs or payouts of NAf. 5,000 or more.
 - o Cumulative-daily rule: A single transaction or a series, combination, or pattern of linked transactions totaling NAf. 5,000 or more within a single gaming day (24-hour period).

Subjective Indicators (Judgment-Based Triggers - Reporting if Suspicion Arises):

These are non-exhaustive examples where there is reasonable cause to presume a transaction is related to ML, TF, or PF (e.g., inconsistent with the player's known profile, source of funds, or behavior). Additional indicators include:

- a) Unexplained large deposits or withdrawals.

- b) Frequent or unusual cryptocurrency exchanges.
- c) Customers attempting to circumvent transaction limits.
- d) Multiple accounts controlled by the same customer.
- e) Unverified third-party payments.
- f) Complex, unusually large transactions, or unusual patterns with no apparent economic or lawful purpose.
- g) Attempts to avoid CDD/KYC (e.g., structuring transactions to stay below thresholds, providing false information, or unusual behavior during verification).
- h) Inconsistent gaming patterns (e.g., minimal play with large deposits/withdrawals, erratic bets, or transfers between accounts without gameplay).
- i) High-risk behaviors such as sudden large bonuses exploitation, frequent wallet changes in crypto transactions, or interactions from high-risk jurisdictions.

Suspicious activities must be reported immediately to the Money Laundering Reporting Officer (MLRO), who will determine whether a Suspicious Activity Report (SAR) / UTR should be filed with relevant authorities in Curacao or the respective jurisdiction of the transaction via goAML.

Reporting Procedures:

- **Internal escalation:** Flag to MLRO with supporting evidence.
- **External reporting:** Submit to FIU via goAML (English preferred) with all details (e.g., player ID, transaction logs, rationale). Bulk reporting allowed for related incidents.
- **Non-submitted UTRs:** Document internally with reasons (retained 5 years).
- **Sanctions/PF integration:** Any sanctions match or PF suspicion triggers immediate UTR/STR to FIU.

3.8 Confirmation of Customer Onboarding and Service Providers

Grace Bay B.V. employs service providers to assist in customer verification and due diligence. Key partners include:

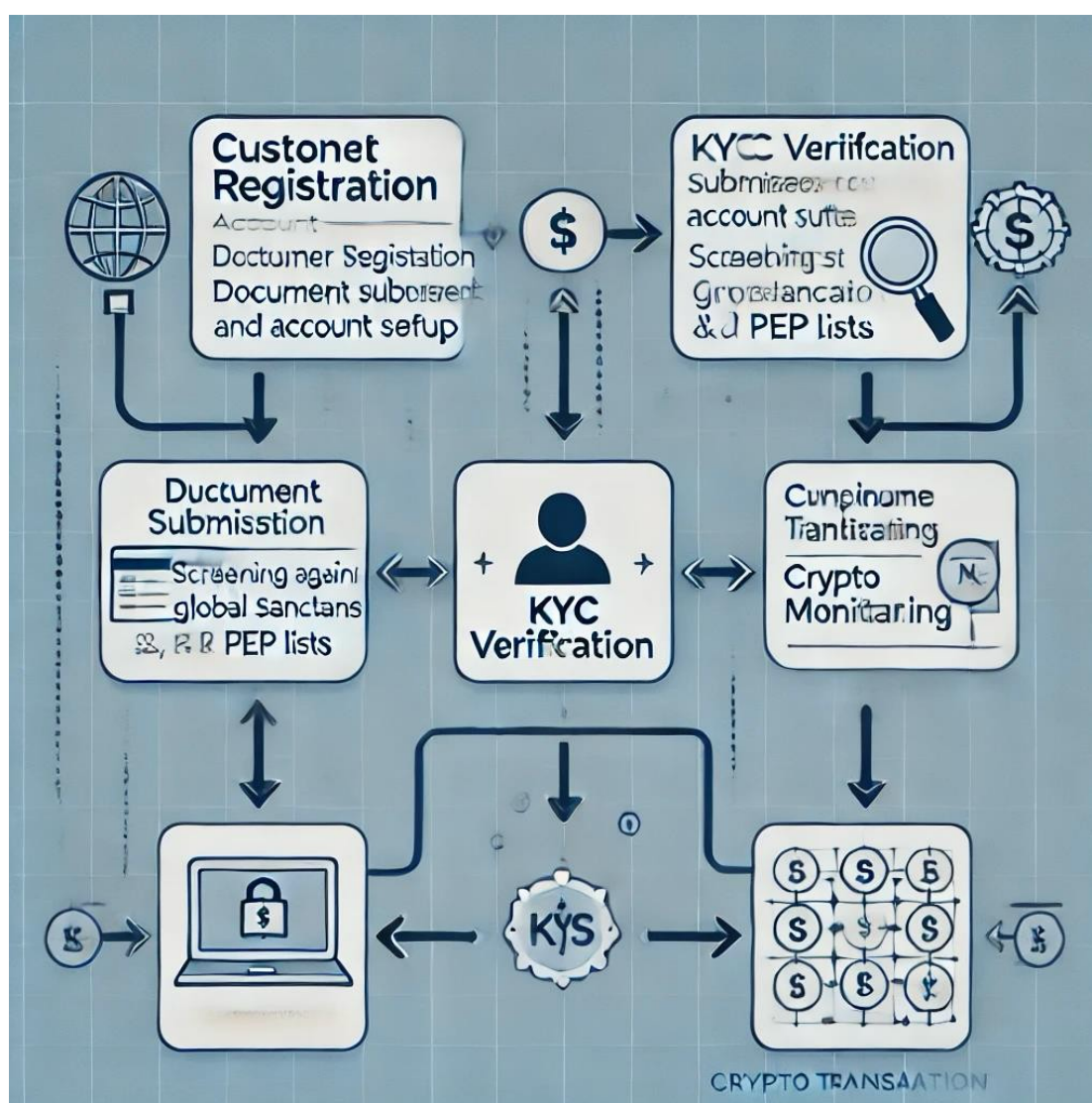
KYC Providers: Verification of customer identification documents and biometric data.

Blockchain Analysis Providers: Monitoring cryptocurrency transactions and assessing the risk of blockchain addresses.

PEP/Sanctions Screening: Cross-checking customers against politically exposed persons (PEPs), sanctions lists, and adverse media databases.

Upon onboarding, each customer must complete the verification process through these service providers. Only after confirmation of successful verification will the customer be allowed to engage in gaming activities or make deposits.

3.9 Structured diagram for Customer Onboarding Process



3.10 MLRO Responsibilities in Customer Onboarding

The Money Laundering Reporting Officer (MLRO) plays a critical role in overseeing the customer onboarding process and ensuring that all AML obligations are met. The key responsibilities of the MLRO during onboarding include:

- Approval of High-Risk Customers:** The MLRO must review and approve all high-risk customer profiles before their account is activated.
- Suspicious Activity Reporting (SAR):** The MLRO is responsible for filing SARs if any suspicious behavior is detected during the onboarding process or at any later stage.
- Ongoing Monitoring:** The MLRO ensures that customer transactions and gaming activity are continuously monitored, especially for high-risk profiles.
- Training & Awareness:** The MLRO is responsible for ensuring that relevant staff are adequately trained on AML regulations and CDD procedures, ensuring compliance across all departments.
- Reporting to Regulators:** The MLRO must report any AML/CFT issues to the Curacao Gaming Authority and relevant global authorities as necessary.

3.11. Record Keeping and Reporting

Grace Bay B.V. is committed to maintaining comprehensive records of all customer transactions and due diligence efforts. These records will be retained for a minimum of 5 years in compliance with Curacao regulations and international best practices. Record-keeping includes:

- A. Customer identification documents.
- B. Transaction details, including the source and destination of funds.
- C. Risk assessments and the rationale for categorizing a customer as low, medium, or high risk.
- D. Any suspicious activity reports (SARs) submitted to relevant authorities.

3.12. Training and Awareness

Grace Bay B.V. will ensure all relevant staff are regularly trained on AML/CFT procedures, customer due diligence requirements, and how to identify suspicious behavior. Training will be conducted at least annually or whenever there are changes in AML regulations or company policy.

The CDD process is designed to ensure that Grace Bay B.V. operates in compliance with the Curacao Gaming Control Board's AML regulations and global AML standards. The comprehensive verification of customer identities, monitoring of transactions, and risk profiling of customers will help the company prevent and mitigate risks associated with money laundering, terrorist financing, and other financial crimes in the online gaming and cryptocurrency space.



4- Know your Customer (KYC), Sanctions Screening & Transaction Monitoring and Reporting

4. Know your Customer (KYC), Sanctions Screening, Transaction Monitoring and Reporting

4.1 Know Your Customer (KYC) System

The Know Your Customer (KYC) system is critical for mitigating risks of money laundering, terrorist financing, and other financial crimes within the online gaming industry. For Grace Bay B.V., which operates under the Curacao Gaming Authority and offers remote gaming services globally, the KYC system must be comprehensive, adaptable to local and global regulations, and designed specifically for the nature of its business.

Grace Bay B.V. prohibits anonymous or fictitious accounts. All accounts require full KYC verification.

4.1.1. Customer Onboarding and Identification Process

Given the nature of Grace Bay B.V.'s business (online gaming, casinos, betting), the onboarding process must be streamlined for a seamless user experience while ensuring strict compliance with AML regulations.

1) Initial Data Collection:

Basic Information: During registration, all customers must provide:

- Full legal name
- Date of birth (confirming they are of legal gambling age, 18+)
- Nationality
- Residential address
- Contact information (email, phone number)
- Unique ID documentation (passport, national ID, or driver's license)

Proof of Identity: Use a reliable document verification process to confirm the customer's identity via the upload of scanned ID documents.

Proof of Address: Customers are required to submit valid proof of address (utility bill, bank statement, government-issued letter) within the last 3 months.

2) Photo Verification:

Live Selfie: Customers must take a live selfie during the onboarding process to ensure they are the legitimate owner of the submitted ID.

Biometric Matching: Biometric technology will be employed to match the live selfie with the ID document photo for authenticity.

3) Age Verification:

Cross-Referencing: Ensure the submitted date of birth and ID document reflect that the customer is of legal gambling age, varying by jurisdiction (but a minimum of 18 years). This is particularly important for jurisdictions with more stringent age-related gaming regulations.

4.1.2. Risk-Based Approach for Customer Classification

The KYC system will use a Risk-Based Approach (RBA), classifying customers into low, medium, and high-risk categories based on various factors, including geographic location, transaction behavior, and the source of funds. This approach aligns with the company's nature of global operations, ensuring compliance with both local Curacao regulations and international standards.

1. Risk Factors Considered:

Geography: Customers residing in high-risk countries (those identified by FATF or subject to international sanctions) will be flagged for Enhanced Due Diligence (EDD). Customers from

jurisdictions with weaker AML regulations will also be subjected to EDD.

Transaction Behavior: Customers who engage in unusually high deposits, frequent withdrawals, or attempts to circumvent KYC requirements (e.g., multiple account registrations) will be flagged as higher risk.

Source of Funds: Customers engaging in crypto transactions will be evaluated based on wallet history and their declared source of funds. Blockchain analytics tools will be used to track the history of crypto transactions for potential illicit activity.

2. Customer Segmentation:

Low-Risk: Customers from stable jurisdictions with low levels of suspicious activity and consistent, modest transaction behavior.

Medium-Risk: Customers with higher transaction volumes or those engaging in crypto-fiat exchanges but operating from low-risk regions.

High-Risk: Customers from high-risk jurisdictions or those showing unusual transactional behavior, inconsistent deposit histories, or questionable sources of funds.

4.1.3. Enhanced Due Diligence (EDD) for High-Risk Customers

For high-risk customers, Enhanced Due Diligence (EDD) will be triggered, requiring more detailed information to prevent potential money laundering and terrorist financing.

Source of Wealth and Funds:

Detailed Declaration: High-risk customers must provide documentation proving their source of wealth and funds (e.g., bank statements, business income records, crypto wallet history).

In-depth Verification: For crypto customers, the KYC system will utilize blockchain analytics tools to assess the risk level of crypto wallets. If any wallet is associated with suspicious activity (e.g., darknet markets, sanctioned countries), onboarding will be rejected.

Frequent Monitoring:

Continuous Screening: High-risk customers are subject to more frequent monitoring. This includes periodic re-verification of identity, source of funds, and transaction scrutiny.

Behavioral Monitoring: The system will track betting patterns, deposit/withdrawal activity, and gaming logs to detect any potential fraud or abuse of bonuses (e.g., bonus hopping).

4.1.4. Crypto-Specific KYC Measures

As Grace Bay B.V. accepts cryptocurrency transactions, the KYC system will incorporate specific procedures to mitigate risks related to crypto's pseudo-anonymity.

Crypto Wallet Registration: Customers must register their crypto wallets before making any deposits. They cannot modify or change wallet addresses without formal approval from the KYC system to prevent identity spoofing or laundering activities through multiple wallets.

Blockchain Analytics: Use blockchain monitoring tools to track wallet activity, assess potential risks, and identify any involvement in illegal activities such as ransomware payments or transactions tied to sanctioned entities.

Source of Crypto Funds: Customers who deposit significant amounts of crypto will be asked to declare the origin of these funds. If the crypto funds have passed through unregulated or high-risk exchanges, further verification will be required.

Transaction Limits: Set daily and monthly deposit and withdrawal limits for both fiat and crypto. Any customer attempting to exceed these limits will trigger an EDD process to ensure the legitimacy of funds and prevent smurfing (breaking large amounts into smaller deposits).

4.1.5. Ongoing Customer Monitoring and Re-verification

Once customers are onboarded, the KYC system will ensure continuous monitoring and periodic re-verification to detect any suspicious behavior or change in risk profile.

Transaction Monitoring:

- 1) The KYC system will integrate with the transaction monitoring system to identify patterns of suspicious activity, such as:
 - a) Sudden spikes in transaction amounts
 - b) Large withdrawals after big wins
 - c) Frequent deposits followed by immediate withdrawals (layering).
- 2) Any flagged transaction will automatically trigger a Suspicious Activity Report (SAR), which the MLRO (Money Laundering Reporting Officer) must review.

Dynamic Risk Scoring:

Customers' risk levels will be dynamically updated based on their behavior and activity. If a customer exhibits consistent low-risk behavior, their risk profile may be downgraded. Conversely, any red flags will lead to EDD and possible account suspension.

Periodic Re-verification:

Customers must undergo periodic re-verification of their identity and source of funds, particularly if their account shows unusual activity or if global regulatory changes demand enhanced compliance.

4.1.6. Geographical Risk Management

Since Grace Bay B.V. operates globally, the KYC system must account for jurisdiction-specific requirements.

High-Risk Jurisdictions:

- a) Customers from FATF-listed countries or regions under increase monitoring will be automatically flagged for EDD. These customers may be restricted from using certain services or subjected to stringent withdrawal and transaction limits.
- b) Jurisdictions with weak AML enforcement will also be flagged for heightened monitoring and controls.

Country-Specific Requirements:

- a) For countries with stricter KYC and AML regulations (e.g., EU, US), the system will adapt to meet local regulatory demands, including additional documentation, increased transaction scrutiny, and mandatory reporting.
- b) Customers operating from countries with robust AML frameworks will undergo simplified due diligence, ensuring compliance while maintaining user experience.

4.1.7 Customer KYC & Control Checks to Minimize Fraud Risk

The following steps Grace Bay B.V. takes to monitor and analyze customer accounts and transactions to ensure a safe, fair, and secure gaming environment for all customers. The procedures implemented aim to minimize fraud risks while ensuring compliance with applicable Anti-Money Laundering (AML) regulations.

Step 1: Fraud & KYC Control: Every customer registering on any of Grace Bay B.V.'s websites is subject to thorough Know Your Customer (KYC) checks. These checks help ensure that all customers are legitimate and are using the platform in a compliant and secure manner.

Step 1.1: Email & Mobile Phone Verifications: Upon registration, customers are required to provide their email address and mobile phone number. These details undergo verification processes to ensure their authenticity and prevent multiple accounts created using false information.

Verification Process: Customers receive an automated email or SMS containing a verification code. They must enter this code to confirm their contact information.

E-mail Activation	Passive
GSM Activation	Passive

Back Office System: Once the verification is complete, the account is updated and marked as verified in our back office system, indicating that the customer has passed the first phase of KYC.

E-mail Activation	Active
GSM Activation	Active

This ensures that customers can only proceed with a valid email address and mobile number, limiting the risk of fraudulent registrations.

Step 1.2: IP Address Checks: To further safeguard against fraudulent activities such as bonus abuse, Grace Bay B.V. conducts comprehensive IP address checks. This helps prevent customers from creating duplicate accounts using different credentials but the same IP address.

Monitoring System: Our system continuously monitors for duplicate or suspicious IP addresses associated with multiple accounts.

Alert System: If any suspicious activity is detected, such as multiple accounts being created from the same IP address, the system immediately flags the issue and alerts the appropriate personnel for investigation.

Id	Username	First Name	Last Name	Email	Activated	Auth Ip	Registration date	Activate
2132011	gokhanh13	Gokhan	Hasan	gokh@*.c	Email GSM	109.71.248.0	2023-09-13 19:24:29	
2132012	sseymaa61	Seymaa	Agar	sey@*.c	Email GSM	109.72.123.16	2023-09-13 19:24:27	
2132013	Metebek4516	Metebek	Kanadli	met@*.c	Email GSM	109.71.251.222	2023-09-13 19:24:21	
2132014	Canbey5757	Can	Onur	can@*.c	Email GSM	98.98.208.0	2023-09-16 19:24:15	
2132015	hamzaason	Hamza	Ayon	ham@*.c	Email GSM	94.156.79.233	2023-09-13 19:24:08	
2132016	Jaguar1x	Eren	Uygun	ere@*.c	Email GSM	194.28.156.13	2023-09-13 19:24:02	
2132017	Hatice1903	Hatice	Uygun	hat@*.c	Email GSM	194.31.79.241	2023-09-13 19:23:53	
2132018	eyoca08	Eyuphan	Yaman	eyu@*.c	Email GSM	45.132.96.138	2023-09-13 19:23:47	
2132019	Mert4322	Mertcan	Yildirim	tam@*.c	Email GSM	185.137.91.3	2023-09-13 19:23:42	
2132020	Erencalik53	Eren	Uygun	ere@*.c	Email GSM	102.129.167.67	2023-09-13 19:23:31	

Member IP Relation

Ip	Member	Date
94.156.79.233	hamzaason	5 hours ago
94.156.79.233	delisvasi58	18 hours ago
94.156.79.233	TS2020	1 day ago
94.156.79.233	Diyarobey	2 days ago

Our back office system also allows for the quick identification of linked accounts and enables prompt action, reducing the potential for fraud.

Step 2: KYC Checks

Grace Bay B.V. is committed to ensuring that its gaming services are provided in a fair and secure manner, while also protecting underage and vulnerable individuals. Customers are required to undergo a comprehensive KYC process to verify their identity and ensure compliance with AML regulations.

Step 2.1: KYC Process

Identity Verification: Customers are required to submit valid identification documents, such as a passport, driver's license, or national ID, as part of the verification process.

Document Submission: Customers can upload their identification documents directly from their accounts to Grace Bay B.V.'s secure servers, where the Compliance team reviews and verifies the information.

Step 3: View from Customer Account:

The screenshot shows a customer's account dashboard. On the left is a sidebar menu with options: Deposit, Withdraw, My Account, Request Call, Change Password, Account verification (highlighted), Bonuses, History, and Messages +6. The main content area is titled 'Account verification' and contains the following text:

TIPOBET reserves the right to request documents from users when necessary. If documents are requested, you will be contacted. You can then confirm your account by uploading two of the documents listed below.

Accepted Valid Documents:

- Driver's license
- ID card
- Passport
- Certificate of residence

Why and on what basis do we collect your Personal Data?
We are aware of the trust our customers have in us. TIPOBET is very clear about why we collect your data. First of all, collecting your information is crucial to providing you with the services and products you want. In addition, your data is used to personalize and improve your experience using our services and to contact you from time to time with important information.

UPDATE YOUR INFORMATION
It is important that the information we hold about you is accurate so that we comply with our legal and regulatory obligations and also to provide you with the best possible service. Therefore, we ask you to ensure that your personal data is always up to date. You can update your personal data at any time from your Account via 'My Account/Update My Account' (if applicable) or by contacting Customer Service.

Below the text is a file upload section with a text input 'Choose file or drop here', a 'Browse' button, and an 'Upload' button. At the bottom, there is a table with two columns: 'Image' and 'Status'.

Step 4: View from Back Office:

Staff can view documents, annotate them, approve or deny them, and communicate with the user as necessary.

This screenshot is identical to the one above, showing the 'Account verification' section from a customer's perspective. It includes the same sidebar menu, text about document requirements, a list of accepted documents, a privacy policy explanation, an update information notice, and a file upload area with 'Image' and 'Status' columns.

4.1.8. Data Protection and Compliance with Global Privacy Laws

KYC data management must comply with global data protection laws, such as GDPR (for European customers) and CCPA (for US customers), ensuring privacy and security.

Data Minimization and Retention: Only the necessary customer data will be collected and stored securely. Data will be retained for 5 years post-termination of the customer relationship, or longer if required by law.

Customer Rights: Ensure customers can access, rectify, or delete their data, as per local data protection laws, while balancing compliance with AML retention requirements.

Encryption and Security: All customer data must be encrypted and stored on secure servers, with access limited to authorized personnel only.

Grace Bay B.V.'s KYC system is designed to balance customer convenience with stringent regulatory compliance, tailored to the specific needs of a global online gaming operator. By implementing a risk-based, crypto-aware approach, the system mitigates AML risks while allowing the company to operate effectively under its Curacao Gaming Authority license and across international markets.

4.2. In-House Sanctions Screening System

Grace Bay B.V. In-House Sanctions Screening System, which covers all AML regulations required by the Curacao Gaming Authority (CGA) and global AML frameworks. It is designed to minimize the risks of money laundering (ML), terrorist financing (TF), fraud, and other financial crimes, specifically with regard to the company's remote gaming activities, crypto transactions, and the international scope of its operations.

The company has an obligation to freeze assets immediately if a customer is identified on any sanctions list (UN/EU/local). No transactions will be processed, and the matter will be reported to the FIU and other authorities.

Any sanctions match triggers a UTR/STR to the FIU via goAML.

Grace Bay B.V. is committed to preventing proliferation financing by screening customers and transactions against relevant sanctions lists (UN/EU/local) and reporting any suspicious activities related to PF to the appropriate authorities. The company has an obligation to freeze assets immediately upon identification of any PF-related risks and to comply with targeted financial sanctions.

4.2.1 Scope of the Sanctions Screening System

Grace Bay B.V.'s sanctions screening system is designed to meet global regulatory requirements and align with the company's business activities, including:

Organizing, marketing, and managing online gaming activities such as sports betting, live casinos, poker, bingos, and lotteries.

Facilitating deposits and withdrawals through both traditional bank transfers and cryptocurrency transactions.

Maintaining compliance with international financial sanctions, Curacao's AML framework, and global AML laws, especially when operating in regions outside of Curacao.

4.2.3 Objectives of Sanction Screening System

Compliance with Curacao Gaming Authority Regulations: The sanctions screening system adheres to Curacao's AML framework, ensuring compliance with Curacao Gaming Authority requirements.

Global AML Compliance: It ensures adherence to AML and Counter-Terrorism Financing (CTF) regulations globally, including adherence to the Financial Action Task Force (FATF) standards.

Minimization of Sanction Risks: Screening against worldwide sanctions lists, such as those from the United Nations, European Union, OFAC (Office of Foreign Assets Control), and other relevant international bodies, to prevent sanctioned individuals or entities from accessing Grace Bay B.V.'s services.

Crypto AML Compliance: Addressing risks specific to cryptocurrency transactions by integrating crypto-related sanctions screening and blockchain monitoring tools.

4.2.4 Key Components of the In-House Sanctions Screening System

1. Automated Screening Software: Grace Bay B.V. utilizes a sophisticated automated sanctions screening software integrated into its compliance platform. This software continuously monitors and screens all customer

accounts and transactions in real-time against a comprehensive set of sanctions lists, ensuring compliance with international AML/CTF regulations.

Global Sanctions Lists Monitored:

- 1) United Nations Security Council Sanctions
- 2) European Union Consolidated List of Sanctions
- 3) OFAC (U.S.) Sanctions List
- 4) UK Sanctions List
- 5) Curacao Government Sanctions List
- 6) Other regional and national sanctions list as required

Screening Frequency:

- 1) Real-time initial screening at registration.
- 2) Daily refresh of sanctions lists for ongoing monitoring.
- 3) Ongoing screening for high-risk transactions, particularly related to cryptocurrency or large volumes of fiat transactions.

4.2.4. Customer Onboarding & Registration Screening

During the onboarding process, each customer is subject to screening to ensure they are not flagged under any sanctions list. This is a critical part of Grace Bay B.V.'s KYC process.

Identity Verification: Customers provide personal details such as full name, date of birth, nationality, and government-issued ID during registration.

Sanctions Screening: The system cross-references customer information with global sanctions databases to detect any matches. Any customer flagged as a positive match will be immediately restricted from further activity until the issue is investigated by the Compliance team.

4.2.3. Ongoing Transactional Screening

Grace Bay B.V. implements continuous transaction monitoring to screen customer deposits, withdrawals, and transfers for any suspicious or high-risk behavior. This includes both fiat and cryptocurrency transactions.

Bank Transactions: All bank transactions are screened to ensure compliance with international financial sanctions. Customer names associated with deposits and withdrawals are cross-checked with sanctions lists.

Crypto Transactions: Cryptocurrency transactions undergo blockchain analysis using Chainalysis, a third-party blockchain monitoring tool. This analysis:

- a) Monitors wallet addresses for links to sanctioned entities or individuals.
- b) Detects illicit activities, such as the use of proceeds from ransomware or other criminal enterprises.
- c) Screens wallet addresses against known risky addresses, including those blacklisted by international bodies or used in darknet activities.

4.2.4. Risk-Based Approach for Screening of High-Risk Customers

Grace Bay B.V. applies a Risk-Based Approach (RBA) to customer profiles and transactions. This helps to prioritize and intensify sanctions screening for high-risk customers based on several factors:

High-risk factors include but are not limited to:

- Customers from high-risk jurisdictions as per FATF recommendations.
- High-value crypto deposits or withdrawals.
- Customers with unusual transaction patterns (e.g., a sudden increase in transaction amounts).
- Customers benefiting from high bonuses or promotions, which may attract bonus abusers or fraudsters.

Enhanced Due Diligence (EDD) is triggered if any of the above risk factors are identified. These customers undergo more thorough sanctions screening, including manual review by the Compliance team and additional identity checks.

4.2.5. Cryptocurrency-Specific Controls

Cryptocurrency poses unique challenges in sanctions screening. Grace Bay B.V. has implemented the following controls to mitigate these risks:

Accepted Cryptocurrencies: The company only accepts widely recognized cryptocurrencies (e.g., Bitcoin, Ethereum). Cryptocurrencies linked to high-risk or sanctioned jurisdictions are prohibited.

Wallet Registration: Customers must register their crypto wallets before initiating deposits. Any changes to wallet addresses are restricted without prior authorization.

Transaction Monitoring: Transactions are analysed for suspicious behavior, such as rapid, large-scale transfers. Any deviation from normal patterns triggers an alert for further investigation.

4.2.6. Internal Reporting and Investigation

Any customer account or transaction flagged by the sanctions screening system is immediately reported to the Compliance team.

Actionable Alerts: The Compliance team receives real-time alerts for any potential matches or suspicious activity.

Manual Review: In the case of false positives or ambiguous results, a manual review is conducted to verify the accuracy of the match.

Internal Reporting: If a confirmed sanctions match is found, the relevant authorities (such as Curacao Gaming Authority or international regulators) are notified, and the customer's account is immediately frozen pending further action.

4.2.7. Ongoing Monitoring and Training

To maintain the effectiveness of the sanctions screening system, Grace Bay B.V. conducts regular reviews of its screening processes and provides ongoing AML/CTF training to staff.

System Updates: The sanctions screening system is updated regularly to include new sanctions lists, emerging threats, and updated regulations.

Staff Training: Compliance staff receive regular training on the use of the sanctions screening system, as well as updates on AML/CTF best practices and regulatory changes.

The In-House Sanctions Screening System developed for Grace Bay B.V. ensures compliance with global AML regulations and Curacao Gaming Authority requirements. By utilizing cutting-edge technology and a risk-based approach, Grace Bay B.V. effectively monitors all customer transactions and accounts, reducing the risk of exposure to sanctioned entities or individuals and preventing the company from being exploited for financial crimes. This comprehensive system provides a solid foundation for expanding operations globally, while maintaining the integrity and security of its remote gaming activities.

4.3 In-House Transactions Monitoring System

4.3.1. System Overview

Grace Bay B.V. has developed an In-House Transactions Monitoring System that complies with the AML regulations of the Curacao Gaming Authority and global standards, aligned with the company's worldwide operations. The system continuously monitors player transactions, deposits, withdrawals, and gameplay behaviors to detect and prevent money laundering, terrorist financing, fraud, and other suspicious activities across Grace Bay B.V.'s domains, Tipobet365.com and Tipobet.com.

4.3.2. Key Features of the Transactions Monitoring System

The system is designed to monitor all types of transactions, particularly focusing on bank and crypto transactions, while ensuring compliance with AML requirements in various jurisdictions. The system is built to detect and prevent suspicious transactions, abnormal behavior, and potential fraud through automated alert triggers.

1) Deposit Monitoring

The deposit monitoring mechanism is designed to flag suspicious deposit patterns. Key aspects of this module include:

Name Mismatch Alerts: If a player deposits funds under a different name from the registered account holder, an alert is generated.

Deposit Form Blank or Incomplete (Bank Transfers): Any blank or incomplete bank transfer forms are flagged for review.

Incorrect Deposit Amount: Deposits made with incorrect or unusual amounts (for both bank and crypto payments) are flagged for further investigation.

Multiple Deposit Methods: When a player uses several deposit methods within a short period, this will trigger an alert for possible structuring or layering in AML terms.

Excessive Deposit Amounts: Deposits significantly above the player's typical range trigger high-risk alerts, especially if they exceed standard daily limits.

2) Withdrawal Monitoring

Grace Bay B.V.'s withdrawal monitoring system ensures that withdrawals align with AML standards. The system checks the following:

Withdrawal to Different Accounts: If the withdrawal is requested to an account not registered with the player, this triggers an immediate alert.

Mismatch in Withdrawal Method: Withdrawals requested via a method different from the one used for deposits trigger an alarm, ensuring consistency in payment methods.

Excessive Withdrawals Relative to Deposits: Withdrawals disproportionate to the amount deposited, particularly when there's little or no gameplay, will flag for AML investigation.

Withdrawal to Different Names: Any withdrawals made to a name other than the registered account holder are flagged.

High-Value Withdrawals: Withdrawals that exceed the player's average amount, especially those close to or above the set limits, trigger alerts.

3) In-Game Behavior Monitoring

The system monitors player behavior during games to detect anomalies that could indicate fraudulent or high-risk activities. Some of the play patterns flagged include:

Unusually High Bets: Bets that are significantly larger than the player's previous betting behavior will trigger an alert.

Low-Risk, High-Volume Betting: Players placing low-risk bets (e.g., red/black in roulette) continuously could be flagged for bonus abuse or AML concerns.

Multiple Wagers on Same Market/Event: Placing multiple similar bets on the same market or event triggers an alert, indicating possible market manipulation or fraud.

Bonus Exploitation: Continuous use of bonus-related offers to exploit the system, such as withdrawing funds immediately after receiving bonuses, is closely monitored.

4) Cryptocurrency Transactions Monitoring

As crypto transactions present unique risks, the system has specific alert categories tailored for cryptocurrency deposits and withdrawals:

Multiple Crypto Addresses: The use of multiple unverified wallets addresses by a player will trigger an alert.

Cryptocurrency Deposit or Withdrawal Rates: Unusually high deposit or withdrawal rates in cryptocurrency trigger alerts, especially if they are disproportionate to the player's usual activity.

Unverified Crypto Wallets: Players must register their crypto wallets before depositing, and any deposit from an unregistered wallet is flagged for review.

Crypto-to-Fiat Exchanges: The system monitors for attempts to convert large amounts of cryptocurrency to fiat currency, especially when the player has not engaged in proportional gaming activities.

4.3.3. Alert System

The alert system operates continuously, providing real-time notifications to the compliance team when suspicious activities occur. Alerts are categorized based on the severity of the risk and the potential for AML breaches. The main categories are:

Deposit Alerts: Triggered by abnormal deposit behavior such as name mismatches, use of multiple deposit methods, or excessive deposit amounts.

Withdrawal Alerts: Triggered by withdrawals that deviate from normal player behavior, including mismatched account names or excessive withdrawal amounts.

In-Game Behavior Alerts: Triggered by unusual gaming patterns, such as excessive betting, bonus abuse, or low-risk betting strategies.

Cryptocurrency Alerts: Specific to cryptocurrency transactions, focusing on multiple wallets, unverified addresses, and abnormal crypto-fiat conversion attempts.

Each alert is assigned a risk level (low, medium, or high) depending on the nature of the activity, allowing the compliance team to prioritize investigations.

4.3.4. AML Detection System

The AML detection system integrates all alerts from various transaction types (deposits, withdrawals, gameplay, and cryptocurrency). When multiple triggers are activated by the same player, their profile is flagged for a comprehensive AML review. This process includes:

Review of Transaction History: The system compiles a history of the player's previous deposits, withdrawals, and game activity to identify patterns indicative of money laundering or terrorist financing.

Review of Player Identification: A secondary verification process checks the player's identity against sanction lists, PEP databases, and adverse media screenings.

Escalation to AML Team: If suspicious activity is confirmed, the case is escalated to the AML team for manual investigation. This includes reviewing all transaction data, verifying the legitimacy of funds, and ensuring compliance with AML regulations.

4.3.5. Crypto Risk Policies

Given that Grace Bay B.V. operates globally and accepts both cryptocurrency and fiat payments, the company has implemented the following crypto risk policies:

Accepted Cryptocurrencies: Only a predefined list of cryptocurrencies (e.g., Bitcoin, Ethereum) is accepted to minimize the risk of dealing with high-risk or anonymous cryptocurrencies.

Wallet Registration: Players must register their cryptocurrency wallets before making any deposits. Wallets are verified, and any changes must be authorized through a secure process.

Crypto-to-Fiat Conversion Limits: Limits are set on the amount of cryptocurrency that can be converted to fiat currency in a single transaction. This helps reduce the risk of large-scale money laundering via crypto channels.

Transaction Monitoring: Every crypto transaction is monitored for suspicious patterns, such as multiple addresses, high-frequency transfers, and the use of mixers or anonymizing services.

The monitoring system ensures compliance with the Curacao Gaming Control Board's AML regulations by:

Customer Due Diligence (CDD): Conducting thorough CDD, including KYC procedures, wallet verification, and regular customer risk assessments.

Ongoing Monitoring: Continuously monitoring customer transactions and behavior for suspicious activities, with alerts triggered based on predefined criteria.

Record Keeping: Maintaining detailed transaction records for each player, including all alerts and investigation outcomes, in compliance with AML regulations.

Reporting to Authorities: Any suspicious transactions are reported to the relevant financial authorities in accordance with Curacao's AML requirements and international guidelines such as FATF.

4.3.6 Failure to Report Suspicious Activity & Suspicious Transaction

Employees of Grace Bay B.V. are required to report any suspicious activities or transactions immediately to the designated compliance team. Failure to do so is a serious breach of AML regulations and may result in penalties, both for the employee and the company. All suspicious transactions, such as unusually large deposits, sudden withdrawals, or inconsistent betting patterns, must be escalated without delay.

4.3.7 Tipping Off

It is strictly prohibited for any staff member to disclose to a customer or third party that their activities are under investigation or being reported for suspicion of money laundering or other illicit activities. "Tipping off" can hinder investigations and is a criminal offense, subject to severe penalties.

Grace Bay B.V.'s In-House Transactions Monitoring System is a robust solution that addresses the complexities of AML compliance in the global remote gaming industry. By integrating real-time alerts, behavior monitoring, and comprehensive AML detection protocols, the system ensures the company adheres to the highest standards of regulatory compliance and risk management.

It is strictly prohibited to tip off customers or third parties about investigations or reports.

The background is a teal-colored image with a blurred effect. It shows a document with lines of text and a keyboard, suggesting a business or office environment.

5- Lines of Reporting s Record Keeping

5. Lines of Reporting & Record Keeping

This section AML policy outlines how Grace Bay B.V. ensures robust lines of reporting and secure record-keeping practices, which are essential for meeting both local and international AML compliance standards.

5.1. Lines of Reporting

Grace Bay B.V. has established a clear and structured reporting line for the identification, escalation, and reporting of suspicious transactions or activities. The process is designed to ensure compliance with AML regulations of the Curacao Gaming Authority (CGA) and international standards.

- 1) **AML Staff:** All AML staff members are required to monitor transactions and customer behavior as part of their day-to-day responsibilities. Any suspicious activity must be reported immediately to the designated Money Laundering Reporting Officer (MLRO).
- 2) **Money Laundering Reporting Officer (MLRO):** The MLRO is responsible for assessing reports of suspicious transactions received from staff. If a transaction or activity is deemed suspicious, the MLRO will escalate it to relevant authorities and law enforcement. The MLRO ensures that reports are compiled accurately, with all supporting documents, before submission to the CGA or international authorities as required.
- 3) **Senior Management:** The MLRO reports directly to senior management on the overall effectiveness of AML measures. Regular updates on suspicious activity reports (SARs) & suspicious Transaction reports (STRs), transaction monitoring results, and regulatory compliance are provided to management for further decision-making.
- 4) **External Authorities:** If suspicious transactions or activities are confirmed, the MLRO must file a SAR & STR with the Financial Intelligence Unit (FIU) of Curacao, or the relevant body based on the location of operation. The company also cooperates fully with requests from law enforcement or regulatory authorities.

5.1.1. Reporting Procedures

- 1) **Suspicious Transaction Reporting (STR):** All employees are trained to recognize red flags related to money laundering and terrorist financing. Upon detection, they report their findings to the MLRO using an internal reporting form.
- 2) **Transaction Thresholds:** Transactions exceeding defined thresholds, such as large crypto or fiat withdrawals, must be automatically flagged and reported to the MLRO for review.
- 3) **Regular Internal Reporting:** The MLRO conducts periodic audits of the company's transaction monitoring systems and AML compliance measures. Findings are compiled in internal reports, which are reviewed by management.

5.2 Record Keeping

To ensure compliance with Curacao Gaming Authority regulations and global AML laws, Grace Bay B.V. maintains detailed records for a minimum period of 5 years, as per international best practices. The following records are kept securely and confidentially:

5.2.1. Customer Due Diligence (CDD) Records:

- Information gathered during the customer onboarding process, including Know Your Customer (KYC) data, identification documents, and proof of address.
- Records of Enhanced Due Diligence (EDD) measures for higher-risk customers, such as those flagged as politically exposed persons (PEPs) or associated with high-risk jurisdictions.

5.2.2 Transaction Records:

- Detailed logs of all transactions, including deposits, withdrawals, and cryptocurrency exchanges, with timestamps, amounts, and account identifiers.
- Cryptocurrency wallet addresses and related details, including source of funds and destination of withdrawals.

5.2.3 Suspicious Transaction Reports (STRs) & Suspicious Activity Reports (SARs):

- Copies of all internal and external STRs & SARs, along with supporting documentation (transaction histories, customer profiles, and any relevant communication).
- Records of decisions made regarding whether or not to escalate reports to the Financial Intelligence Unit (FIU) or other international regulatory bodies.

5.2.4 Internal and External Audit Reports:

- Regular audit reports on the effectiveness of AML controls, systems, and compliance measures.
- Documentation of corrective actions taken in response to identified gaps or non-compliance issues.

5.2.5 Communication Records:

All correspondence with regulatory authorities, including responses to information requests, compliance reviews, or investigations.

5.2.6 Employee Training Records:

Detailed logs of AML training sessions, including attendance records, training materials, and certifications of completion.

5.2.7. Data Security and Confidentiality

Grace Bay B.V. ensures that all records are stored in a secure manner, whether digitally or physically, and are only accessible to authorized personnel. The company follows strict data protection policies to comply with international data privacy laws (e.g., GDPR) and prevent unauthorized access to sensitive information.

Digital Records: Transaction logs and customer data are stored on secure servers with encrypted access. Backup copies are maintained to ensure records are not lost due to system failures or breaches.

Physical Records: If any documents are stored physically, they are kept in secure, locked locations accessible only by the MLRO and senior compliance personnel.

5.2.8. Disposal of Records

After the mandatory record retention period (5 years), Grace Bay B.V. will securely dispose of customer and transaction records. Disposal processes include the permanent deletion of digital records and the shredding of physical documents to ensure no unauthorized retrieval of sensitive data.

5.3. Internal Controls

- **Internal controls include customer acceptance policies (CAP):** Acceptance based on low/medium risk after CRA, decline for unmitigated high risk (as per Reg. V.2).
- **Sanctions compliance:** As detailed in 4.2.
- **Transaction monitoring design:** Real-time, risk-based, with alerts as in 4.3.
- **Recordkeeping:** Aligned with regulation, including internal logs for non-submitted UTRs (retained 5 years).
- **Employee screening program:** All employees are screened for criminal records, sanctions, financial suitability before hiring and annually (as per Reg. V.4).

Grace Bay B.V. commits to full cooperation with CGA examinations, providing documents and access (as per Reg. V.6).

A blurred background image of a large audience in a hall, with a person in the foreground holding a microphone. The person is seen from the side, wearing a dark suit, and is holding a black microphone. The audience is out of focus, showing many people seated in rows. The lighting is warm and slightly dim, typical of an indoor event.

6- Training and Awareness

6. Training and Awareness

To ensure full compliance with Anti-Money Laundering (AML) regulations under the Curacao Gaming Authority (CGA) and international standards, Grace Bay B.V. has implemented a comprehensive Training and Awareness Program. This program ensures that all employees are fully informed and equipped to identify, prevent, and report suspicious activities related to money laundering and terrorist financing, particularly in the context of the company's online gaming operations.

Employee screening is integrated into onboarding training.

6.3. General Training Requirements

Grace Bay B.V. requires all employees, regardless of their position, to undergo AML training at regular intervals. The training program is designed to meet the specific requirements of the Curacao Gaming Control Board, global AML regulations, and the nature of the company's business, which includes remote gaming activities like betting exchanges, interactive casinos, lotteries, and cryptocurrency transactions.

6.2 Training Frequency:

Initial Training: Provided to all new employees during onboarding, ensuring they understand the company's AML policy, reporting obligations, and regulatory requirements.

Ongoing Training: Conducted annually for all employees to update them on regulatory changes, emerging risks, and developments in AML procedures.

Targeted Training: Additional training for employees working in high-risk areas (e.g., customer onboarding, transactions, and cryptocurrency-related operations) or when there are significant changes to AML regulations or company operations.

6.4. Training Content

The AML training provided by Grace Bay B.V. covers the following essential areas:

Understanding Money Laundering and Terrorist Financing:

- 1) The nature, methods, and stages of money laundering (placement, layering, and integration).
- 2) How terrorist financing can occur in the context of online gaming.

Regulatory Framework:

- 1) Overview of the Curacao Gaming Authority AML regulations.
- 2) International AML standards, such as those set by the Financial Action Task Force (FATF).
- 3) Specific requirements for companies handling cryptocurrency, including regulations in key markets like Europe, North America, and Asia.

Company-Specific AML Policies:

- 1) Grace Bay B.V.'s AML policy, including the process for conducting Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD).
- 2) How the company monitors customer transactions, including both fiat and cryptocurrency transactions.
- 3) Procedures for reporting suspicious activities to the Money Laundering Reporting Officer (MLRO).

Cryptocurrency and AML:

- 1) How cryptocurrency can be used in money laundering and the company's specific policies for preventing its misuse.
- 2) The types of cryptocurrencies accepted by Grace Bay B.V. and the process for converting cryptocurrency to fiat.
- 3) Monitoring and reporting requirements for large or unusual cryptocurrency transactions.

Recognizing Suspicious Activities:

- 1) Red flags in customer behavior, such as large deposits, unusual transaction patterns, or frequent bonus claims.
- 2) How to identify suspicious activity related to in-game purchases or cryptocurrency transactions.
- 3) The process for escalating suspicious transactions or activities internally to the MLRO.

Tipping Off and Confidentiality:

- 1) Employees are trained on the prohibition of tipping off, which involves alerting a customer that their transaction has been flagged or reported.
- 2) The importance of maintaining the confidentiality of suspicious transaction reports (STRs) and investigations.

Risk-Based Approach (RBA):

- 1) How employees can assess the risk of money laundering and terrorist financing based on customer profiles and transaction types.
- 2) How the company's risk-based approach influences decisions about Enhanced Due Diligence (EDD) for high-risk customers, such as those with large or sudden deposits, or from high-risk countries.

6.5. Role-Specific Training

Certain roles within Grace Bay B.V. require more specialized AML training:

Customer Service Staff:

- 1) Trained on how to handle customer inquiries related to deposits and withdrawals, particularly concerning cryptocurrency transactions.
- 2) Understanding of how to verify customer identity and detect discrepancies between account information and transaction details.

Financial and Transaction Monitoring Teams:

- 1) Provided with in-depth training on transaction monitoring tools and how to review and assess transaction logs for suspicious activity.
- 2) Specific focus on the handling of large cryptocurrency transactions and unusual betting patterns.

MLRO and Compliance Officers:

- 1) Regular training on regulatory updates, the evolving risk landscape, and the specific responsibilities of an MLRO under Curacao and international law.
- 2) Advanced knowledge of preparing and submitting Suspicious Transaction Reports (STRs) to the relevant authorities.

6.6. AML Awareness Campaigns

To foster a culture of compliance within the organization, Grace Bay B.V. conducts regular awareness initiatives, including:

Internal Bulletins: Periodic updates sent to all employees to highlight changes in AML regulations, emerging money laundering risks in the gaming and cryptocurrency sectors, and key case studies.

Workshops and Seminars: Engaging and interactive sessions where employees can discuss real-world AML scenarios, review current cases, and share best practices.

Online Learning Modules: Employees can access an e-learning portal with various modules on AML topics, tailored to different roles within the company. Completion of these modules is tracked, and employees are tested to ensure comprehension.

6.7. Evaluation and Continuous Improvement

Grace Bay B.V. continuously evaluates the effectiveness of its AML training program through:

Feedback Mechanisms: Employees are encouraged to provide feedback after training sessions, allowing the company to improve the content and delivery of future training.

Testing and Certification: Employees undergo periodic testing after completing training to ensure they understand AML regulations and company policies. Certification is provided for those who successfully pass the tests.

Regular Audits: The MLRO and Compliance Team audit the training program annually to ensure it aligns with current regulations and the company's evolving business model. Any gaps identified are addressed through targeted training initiatives.

6.8. Reporting and Documentation of Training

All training sessions, including attendance records and training materials, are documented and securely stored by the Compliance Team. This ensures that the company can provide proof of compliance to regulators, such as the Curacao Gaming Control Board, during audits or investigations.

This comprehensive Training and Awareness Program ensures that Grace Bay B.V. staff are well-prepared to prevent, identify, and report any activities related to money laundering or terrorist financing, in compliance with both Curacao and international regulations. The focus on role-specific training, cryptocurrency risks, and ongoing awareness initiatives supports the company's commitment to maintaining the highest standards of AML compliance.