



Grace Bay B.V. Crypto Risk Policies

Table of Contents

1. Introduction	6
1.1. Objectives	6
1.2. Key Components of Our Crypto Risk Policy	6
1.2.1. Risk-Based Approach to Identifying and Mitigating ML/TF Risks	6
1.2.2. Acceptance of Cryptocurrencies for Deposits and Withdrawals	6
1.2.3. Crypto Risk Policy on Updating Accepted Cryptocurrencies	7
1.2.4. Anti-Money Laundering (AML) Measures	7
1.2.5. Cryptocurrency Wallet Registration and Verification	8
1.2.6. Monitoring of Crypto-to-Fiat Exchanges	8
1.2.7. Provably Fair Gaming	8
1.2.7. Global Compliance	8
1.2.8. Customer Profile and Limits	9
1.2.9. In-Game Purchases and Monitoring	9
1.2.10. Transaction Volume	9
2. Global Crypto Regulations	11
2.1. Financial Action Task Force (FATF) Guidelines	11
2.2. European Union (EU) Directives	11
2.3. United States Regulations FinCEN Guidelines	12
2.4. United Kingdom (FCA) Guidelines	12
2.5. I Gaming Crypto Regulations	12
3. Crypto AML Compliance Measures	14
3.1. Objective	14
3.2. Review Frequency	14
3.3. Cryptocurrency Regulations Worldwide	14
3.4. Risk Based Approach	15
3.4.1. Type of Customers and Their Activities	15
3.4.2. The Countries or Geographic Areas in Which the Company Does Business	15
3.4.3. Customer Risk Assessment	15
3.4.4. Transaction Risk Management	16
3.4.5. Services Risk (Product & Service Risk Factors)	16
3.4.6. Geographical Risk and Jurisdictional Exposure	16
3.4.7. Cryptocurrency Risk Management	16

3.4.8. Delivery Channel Risk.....	17
3.4.9. Commitment to Managing Transaction Risks.....	17
3.4.10. Mitigation Measures	17
4. Customer Due Diligence (CDD)	19
4.1. CDD Objectives	19
4.2. When CDD is Required	19
4.3. CDD Procedures	19
4.3.1. Identification and Verification	19
4.3.2. Customer Risk Profiling	19
4.3.3. Ongoing Monitoring	20
4.4. Enhanced Due Diligence (EDD)	20
4.5. Simplified Due Diligence (SDD)	20
4.6 Failure to Conduct Customer Due Diligence	20
4.7. Suspicious Activity Reporting (SAR)	21
5. Know your Customer (KYC), Sanctions Screening, Transaction Monitoring and Reporting.....	23
5.1 Know Your Customer (KYC) System	23
5.1.1. Customer Onboarding and Identification Process.....	23
5.1.2. Crypto-Specific KYC Measures	23
5.1.3 Customer KYC & Control Checks to Minimize Fraud Risk.....	24
5.2. In-House Sanctions Screening System.....	26
5.2.1 Objectives of Sanction Screening System	26
5.2.2 Key Components of the In-House Sanctions Screening System.....	26
5.2.3. Customer Onboarding & Registration Screening.....	26
5.2.4. Ongoing Transactional Screening.....	27
5.2.5. Cryptocurrency-Specific Controls	27
5.2.6. Internal Reporting and Investigation.....	27
5.3 In-House Transactions Monitoring System.....	28
5.3.1. Key Features of the Transactions Monitoring System	28
5.3.2. Alert System	29
5.3.3. AML Detection System	29
6. Lines of Reporting & Record Keeping.....	31
6.1. Lines of Reporting	31
6.1.2 AML Staff.....	31
6.1.2 Senior Management.....	31

6.1.3 External Authorities	31
6.2 Record Keeping	31
6.2.1. Customer Due Diligence (CDD) Records:.....	31
6.2.2 Transaction Records:	31
6.2.3 Suspicious Transaction Reports (STRs) & Suspicious Activity Reports (SARs).....	31
6.2.4 Internal and External Audit Reports	32
6.2.5 Communication Records:	32
6.2.6 Employee Training Records:	32
6.2.7. Data Security and Confidentiality	32
6.2.8. Disposal of Records.....	32
7. Training and Awareness	34
7.1. General Training Requirements	34
7.2 Training Frequency:	34
7.3. Reporting and Documentation of Training	34

A photograph of two business professionals in suits shaking hands. The person on the left is wearing a dark suit, and the person on the right is wearing a light-colored, patterned suit. They are standing in front of a blurred city skyline with tall buildings under a bright sky. The text "1. Introduction" is overlaid in white on the lower left of the image.

1. Introduction

1. Introduction

Grace Bay B.V. is a company registered under the Curacao commercial register and Curacao Gaming Control Board. Our company organizes, markets, promotes, manages, supports, and operates all types of remote gaming activities, including interactive casinos, bingos, lotteries, and other interactive games for clients outside of Curacao. This document outlines the crypto risk policies for our B2C and B2B operations to comply with Crypto AML regulations set by the Curacao Gaming Control Board and other global regulators.

1.1. Objectives

- Prevent money laundering and terrorist financing through the use of cryptocurrency.
- Ensure compliance with Curacao Gaming Control Board regulations and global Crypto AML standards.
- Safeguard the integrity of our online gaming operations.
- Provide clear guidelines for the acceptance, exchange, and monitoring of cryptocurrency transactions.

1.2. Key Components of Our Crypto Risk Policy

1.2.1. Risk-Based Approach to Identifying and Mitigating ML/TF Risks

Grace Bay adopts a Risk-Based Approach (RBA) to manage and mitigate the risks of money laundering and terrorist financing (ML/TF) associated with cryptocurrency transactions. This approach tailors the level of scrutiny and control based on the assessed risk level of individual transactions or customers.

Customer Risk Profiling: Customers are classified based on their risk level (e.g., low, medium, high) considering factors such as transaction volume, geographical location, and behavior. Higher-risk customers are subject to additional verification steps and monitoring.

Transaction Monitoring: Cryptocurrency transactions are monitored in real-time for suspicious activity, including large or sudden transactions, repeated crypto-to-fiat conversions, or connections to high-risk jurisdictions (e.g., sanctioned countries).

Enhanced Controls for High-Risk Transactions: Transactions deemed higher risk may trigger enhanced due diligence measures, such as deeper investigation into the source of funds or transaction history.

This risk-based approach ensures that Grace Bay focuses its resources on the highest-risk transactions, while maintaining compliance with international AML/CFT standards.

1.2.2. Acceptance of Cryptocurrencies for Deposits and Withdrawals

Grace Bay B.V. now accepts a broader range of cryptocurrencies, including Bitcoin (BTC), Litecoin (LTC), Dash (DASH), Dogecoin (DOGE), Bitcoin Cash (BCH), Ravencoin (RVN), USDC (USDC), BitTorrent (BTT), Tron (TRX), Toncoin (TON), Monero (XMR), and USDT (Tether) for transactions. Each cryptocurrency brings unique benefits and risk management considerations, enabling diversified and flexible transaction methods for our clients.

USDT (Tether)

USDT (Tether) is a stablecoin designed to maintain a stable value equivalent to \$1 USD. It is widely used in the cryptocurrency market as a stable asset for trading and transactions.

Reasons for Acceptance:

- **Stability:** USDT's value is pegged to the US dollar, providing a stable alternative to the high volatility typically associated with other cryptocurrencies. This stability is crucial for minimizing the risk of large

fluctuations in transaction values.

- **Liquidity:** USDT has high liquidity, meaning it can be easily converted into fiat currency or other cryptocurrencies with minimal price impact. This liquidity ensures that funds can be quickly and effectively moved in and out of the system without significant delays or complications.
- **Market Acceptance:** USDT is one of the most widely used stablecoins in the cryptocurrency market. Its broad acceptance across various trading platforms and exchanges ensures that transactions using USDT are well-supported and recognized.
- **Traceability:** Despite being a stablecoin, USDT transactions are recorded on a blockchain, allowing for transparency and traceability. This feature helps in monitoring and investigating transactions to prevent money laundering and terrorist financing activities.

Bitcoin (BTC)

- Overview: Bitcoin is the world's first decentralized digital currency, widely recognized and accepted globally.

Reasons for Acceptance:

- Market Dominance: As the most widely traded and recognized cryptocurrency, Bitcoin ensures ease of conversion and high liquidity.
- Transparency: Bitcoin transactions are publicly recorded on the blockchain, ensuring traceability and supporting AML compliance.

Litecoin (LTC)

- Overview: Litecoin is a peer-to-peer cryptocurrency offering faster transaction confirmation times compared to Bitcoin.

Reasons for Acceptance:

- Transaction Speed: Litecoin's fast block generation time makes it suitable for quick deposits and withdrawals.
- Market Acceptance: Well-recognized and accepted across many exchanges and platforms.

Dash (DASH)

- Overview: Dash offers privacy-focused features and faster transactions than Bitcoin.

Reasons for Acceptance:

- Speed: With its InstantSend feature, Dash provides near-instant transaction confirmations.
- Anonymity Options: While enabling fast transactions, Dash can offer optional privacy, suitable for certain user preferences, though this will require enhanced due diligence.

Dogecoin (DOGE)

- Overview: Initially created as a meme currency, Dogecoin has grown into a highly liquid and well-accepted cryptocurrency.

Reasons for Acceptance:

- Community Support: Dogecoin has a large user base and a strong market presence, contributing to high

liquidity.

- Transaction Speed: Fast and efficient for small-value transactions.

Bitcoin Cash (BCH)

- Overview: Bitcoin Cash is a fork of Bitcoin, optimized for lower fees and faster transactions.

Reasons for Acceptance:

- Efficiency: Lower fees and quicker transaction processing make it attractive for online gaming environments.

Ravencoin (RVN)

- Overview: Ravencoin is a blockchain built to handle asset transfers.

Reasons for Acceptance:

- Asset Transfer Capabilities: Its focus on asset and token transfer adds flexibility to the types of value exchanged.

USDC (USD Coin)

- Overview: USDC is a stablecoin fully backed by U.S. dollars, offering stability similar to USDT.

Reasons for Acceptance:

- Stability: Like USDT, USDC provides a stable value pegged to the U.S. dollar.
- Regulatory Transparency: USDC issuers comply with regular audits and transparency standards.

BitTorrent (BTT)

- Overview: BitTorrent Token is a cryptocurrency based on the Tron blockchain, designed to support decentralized file-sharing services.

- **Reasons for Acceptance:**

- Decentralization Focus: BitTorrent's link to decentralized networks aligns with innovative technological developments.

Tron (TRX)

- Overview: Tron is a blockchain-based decentralized platform focusing on content sharing and decentralized applications (dApps).

- **Reasons for Acceptance:**

- Low Transaction Fees: TRX offers affordable transaction costs, making it ideal for frequent or small-value transactions.
- Scalability: Tron's blockchain offers high transaction throughput, supporting multiple users simultaneously.

Toncoin (TON)

- Overview: Toncoin is the cryptocurrency of The Open Network (TON), a blockchain system designed for fast and secure transactions.
- **Reasons for Acceptance:**
- Transaction Speed and Efficiency: Toncoin's infrastructure is optimized for low-latency, high-volume transaction processing.

Monero (XMR)

- Overview: Monero is a privacy-oriented cryptocurrency, offering secure and untraceable transactions.
- **Reasons for Acceptance:**
- Privacy: Monero provides enhanced anonymity through its use of stealth addresses and ring signatures.
- Enhanced Due Diligence: Because of its privacy focus, Monero transactions will require stricter scrutiny and compliance checks to prevent misuse for illicit activities.

1.2.3 Crypto Risk Policy on Updating Accepted Cryptocurrencies

Grace Bay B.V. will continue to monitor and review the acceptance of additional cryptocurrencies to ensure alignment with evolving market conditions and regulatory frameworks. Each cryptocurrency undergoes rigorous evaluation to ensure it aligns with our AML/CFT obligations and supports a secure and compliant operational environment.

Market Developments: The cryptocurrency market is constantly evolving, with new stablecoins or regulatory changes that may influence the decision to accept or reject certain cryptocurrencies. Regular reviews help the company stay aligned with market trends and innovations.

Compliance with AML Regulations: The regulatory landscape for cryptocurrencies is dynamic. Grace Bay B.V. ensures that its cryptocurrency acceptance policy aligns with current AML regulations and standards. If new regulations impact the risk profile of USDT or other potential cryptocurrencies, the list may be updated accordingly.

Through concentrating exclusively on USDT, Grace Bay B.V. simplifies its cryptocurrency handling and risk management while ensuring stability and compliance with AML regulations. The ability to update the policy reflects a proactive approach to maintaining a secure and compliant cryptocurrency environment.

1.2.4. Anti-Money Laundering (AML) Measures

Our AML measures are designed to detect and prevent suspicious activities related to money laundering and terrorist financing.

KYC/AML Procedures for Crypto Customers

Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures are critical for ensuring that all customers using cryptocurrency for transactions are thoroughly vetted before conducting any business. The policy includes specific steps that must be taken for cryptocurrency transactions:

- 1) **Identity Verification:** Every customer must undergo identity verification before transacting in cryptocurrencies. This includes verifying personal information such as names, addresses, dates of birth, and ID documents.
- 2) **Customer Due Diligence (CDD):**
 - a. Verify the identity of customers through government-issued identification.

- b. Ensure that the name on the bank transfer matches the registered name of the player.
 - c. Require customers to register their wallet address before depositing and prohibit changes to this address.
- 3) **Enhanced Due Diligence (EDD):** For high-risk customers or transactions above certain thresholds, Grace Bay applies Enhanced Due Diligence, which requires more in-depth investigation into the customer's identity and the source of their funds.
- 4) **Transaction Monitoring:**
 - a. Monitor transaction patterns and flag unusual or large transactions for further review.
 - b. Analyze game logs to detect irregularities, such as bonus transfers to different accounts or fraudulent activities.
 - c. Set deposit and withdrawal limits to mitigate the risk of large, suspicious transactions.

The purpose of KYC/AML procedures is to prevent individuals or entities involved in illegal activities from using the platform for financial transactions, thereby reducing the risk of money laundering and terrorist financing.

1.2.5. Cryptocurrency Wallet Registration and Verification

One of the key risk areas in cryptocurrency transactions is the anonymity of wallet addresses. Grace Bay requires all customers to register and verify their cryptocurrency wallets before any deposits or withdrawals can be made.

Wallet Registration: Customers must register their cryptocurrency wallet addresses with the Company before making deposits or withdrawals. This ensures that the Company has traceable links between the customer and their wallet.

Wallet Verification: The registered wallet must undergo verification, which may involve blockchain analytics tools to check if the wallet has been linked to any illicit activity in the past. Once verified, customers are not allowed to change their wallet addresses without going through another verification process.

This control ensures that each transaction is conducted through a known and verified wallet, reducing the risk of stolen or fraudulent wallets being used for transactions.

1.2.6. Monitoring of Crypto-to-Fiat Exchanges

Grace Bay B.V. allows customers to convert cryptocurrency to fiat currency, and vice versa, for use in gaming activities. Crypto-to-fiat exchanges pose a significant risk for money laundering, as they provide an opportunity to introduce potentially illicit funds into the traditional financial system.

Monitoring Process: The company actively monitors all crypto-to-fiat exchanges. Large, irregular, or frequent conversions may trigger alerts for further investigation, particularly if the customer's transaction history shows a sudden spike in activity.

Limits on Conversions: The policy sets clear limits on how much cryptocurrency can be exchanged for fiat in a given time period, ensuring that large transactions cannot occur without additional scrutiny.

Monitoring these exchanges helps detect and prevent attempts to launder large sums of cryptocurrency by converting them into fiat currency, especially if linked to illicit activities.

1.2.7. Provably Fair Gaming

We ensure the fairness of our games through blockchain technology, which allows for transparent and verifiable game outcomes. This fosters trust and reduces the risk of manipulation.

Fiat Gambling vs. Blockchain Gambling

- **Fiat Gambling:** Traditional currency transactions are processed through bank transfers. We ensure that the name on the bank account matches the registered name of the player.
- **Blockchain Gambling:** Cryptocurrency transactions are processed through registered wallet addresses. We require customers to register their wallet address and monitor transaction patterns.

1.2.7. Global Compliance

Grace Bay B.V. adheres to the AML regulations of the Curacao Gaming Control Board, which governs its gaming license. Additionally, the Company ensures compliance with international standards for AML and CFT, including guidelines from organizations like the Financial Action Task Force (FATF).

Curacao GCB Requirements:

The policy outlines the specific reporting, record-keeping, and customer due diligence requirements mandated by the Curacao Gaming Control Board for cryptocurrency transactions.

International Standards:

Grace Bay also aligns its AML policy with international best practices, including compliance with FATF recommendations and the laws of the jurisdictions in which it operates globally.

Country Acceptance:

We operate globally, except in countries where online gambling is prohibited. Our operations comply with the legal requirements of each jurisdiction.

Regulatory Requests:

We provide detailed reports on our crypto policies to regulators upon request. These reports include information on accepted cryptocurrencies, AML measures, and transaction monitoring procedures.

By adhering to both local and international standards, Grace Bay ensures that it meets the highest regulatory expectations, regardless of where its customers are located.

1.2.8. Customer Profile and Limits

Demographics:

Our typical customers are men aged 25-32 years old.

Transaction Limits:

We do not serve high net worth individuals. Daily deposit and withdrawal limits are set to manage risk.

Bonuses:

High-risk customers may be attracted by bonuses such as the 100% first deposit bonus. We monitor these customers closely to prevent fraud.

1.2.9. In-Game Purchases and Monitoring

Deposit Checks:

Verify that the transfer method matches the registered details of the player.

- For bank transfers, ensure the player's name matches the account holder's name.
- For crypto transactions, verify the registered wallet address.

Game Log Analysis:

Review game logs to detect any irregularities, such as sudden large transactions or fraudulent activity.

Previous Deposits:

Compare current deposits with previous transactions to identify any significant changes in behavior.

1.2.10. Transaction Volume

- **Daily Volume:** Our total volume for all games is approximately \$50,000 - \$100,000 USD daily, with 2,000 - 4,000 transactions.
- **Transaction Monitoring:** We continuously monitor transaction volume and patterns to detect and prevent suspicious activities.

A glowing crystal ball with a world map inside, sitting on a black base, with a bokeh background of warm lights.

2. Global Crypto Regulations

2. Global Crypto Regulations

Grace Bay B.V., operating under the Curacao Gaming Control Board, must adhere to both local and international regulations for cryptocurrency transactions. These regulations aim to prevent money laundering, terrorist financing, and ensure consumer protection. Below is a detailed explanation of the regulatory requirements specific to Grace Bay B.V. based on its operational jurisdiction and the nature of its business.

2.1 Financial Action Task Force (FATF) Guidelines

Travel Rule

The FATF's Travel Rule mandates that Grace Bay B.V. collect and share specific customer information during cryptocurrency transactions, akin to the requirements for wire transfers in traditional banking. This includes the originators and beneficiary's names, account numbers, and transaction details. Grace Bay B.V. will ensure that its systems are capable of collecting and securely transmitting this information to comply with the Travel Rule. This involves implementing protocols for data collection and secure information sharing to meet FATF standards.

Customer Due Diligence (CDD) and Know Your Customer (KYC) Procedures

Grace Bay B.V. perform comprehensive Customer Due Diligence (CDD) and Know Your Customer (KYC) procedures. This involves verifying the identities of customers using reliable, independent sources such as government-issued identification. For ongoing relationships, Grace Bay B.V. must monitor transactions to detect suspicious activities. This monitoring should be supported by automated systems that flag irregular transactions for further review, ensuring adherence to FATF guidelines.

Monitoring Transactions for Suspicious Activity

Grace Bay B.V. monitor transactions for suspicious activities and report such activities to the relevant authorities. Grace Bay B.V. implemented robust transaction monitoring systems that can detect anomalies or unusual patterns indicative of potential money laundering or terrorist financing. This involves establishing protocols for investigating flagged transactions and ensuring that suspicious activity reports are filed with appropriate regulatory bodies as required.

Record Keeping

Grace Bay B.V. maintain records of transactions and customer information for at least five years. Grace Bay B.V. ensure that all transaction records, including details of the customer, transaction amounts, and dates, are securely stored and easily retrievable. This record-keeping is crucial for enabling audits, investigations, and ensuring compliance with FATF regulations.

2.2 European Union (EU) Directives

5th Anti-Money Laundering Directive (5AMLD)

- The 5th Anti-Money Laundering Directive (5AMLD) extends AML/CTF obligations to cryptocurrency exchanges and wallet providers. As Grace Bay B.V. operates both as a B2C and B2B online gaming company accepting cryptocurrencies, including USDT, it falls under this directive. Grace Bay B.V. must ensure compliance with AML/CTF regulations applicable to cryptocurrency exchanges and wallet providers to prevent the misuse of its services for illicit purposes.
- Under 5AMLD, Grace Bay B.V. is required to implement strict CDD and KYC procedures. For transactions over €1,000, Grace Bay B.V. must verify customer identities using reliable sources, such as government-issued identification. This involves collecting personal information and performing ongoing monitoring of business relationships to detect and prevent suspicious activities.

6th Anti-Money Laundering Directive (6AMLD)

- The 6th Anti-Money Laundering Directive (6AMLD) expands the list of predicate offenses for money laundering to include cybercrime and environmental crime. Grace Bay B.V. must be vigilant in identifying transactions related to these offenses and incorporate this extended scope into its AML policies and procedures.
- 6AMLD provides a unified definition of money laundering across EU member states. Grace Bay B.V. must align its AML practices with this harmonized definition to ensure consistent application of anti-money laundering measures across jurisdictions where it operates.
- The directive holds companies accountable for failing to prevent money laundering within their operations. Grace Bay B.V. establish comprehensive internal controls and procedures to mitigate AML risks and ensure that all employees understand their responsibilities in preventing and reporting money laundering activities.

2.3 United States Regulations FinCEN Guidelines

Under FinCEN regulations, cryptocurrency exchanges and administrators are classified as Money Services Businesses (MSBs). Grace Bay B.V., as a company dealing with cryptocurrencies and online gaming, must adhere to MSB requirements. This classification mandates that Grace Bay B.V. registers with FinCEN, ensuring that the company meets all regulatory obligations related to anti-money laundering (AML) and combating the financing of terrorism (CFT).

2.4 United Kingdom (FCA) Guidelines.

Grace Bay B.V., as an entity dealing with cryptocurrencies and operating in online gaming, must be registered with the Financial Conduct Authority (FCA) if it conducts regulated activities in the UK. This involves submitting an application for registration and complying with FCA requirements. Although Grace Bay B.V. is based in Curacao, if it serves UK customers or has any operations in the UK, FCA registration is necessary to ensure regulatory compliance.

2.5 I Gaming Crypto Regulations

Grace Bay B.V. ensure that it strictly adherence to both local and international iGaming and cryptocurrency regulations. This includes acquiring and maintaining all necessary licenses, such as the Curacao Gaming Control Board license, and complying with applicable financial regulations in the jurisdictions where the company operates.



3. Crypto AML Compliance Measures

3. Crypto AML Compliance Measures

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

3.1 Objective

The primary objectives of Crypto AML Compliance Measures are to:

1. Prevent the use of Grace Bay B.V.'s gaming platforms for money laundering, terrorist financing, or fraudulent activities.
2. Ensure compliance with global Crypto AML regulations as well as the Curacao Gaming Control Board's (GCB) 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.

3.2 Review Frequency

Grace Bay B.V. is committed to maintaining an up-to-date and effective Crypto Anti-Money Laundering (AML) measure in compliance with the regulations of the Curacao Gaming Control Board (GCB) and global standards, including:

We conduct reviews according to the following schedule:

Annually: we 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:

1. Curacao Gaming Control Board regulations and guidance.
2. Global Crypto AML laws, including updates from the Financial Action Task Force (FATF), 5AMLD, and USA Patriot Act, or any other applicable international frameworks.
3. 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.

3.3. 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.

3.4. Risk Based Approach

The Risk-Based Approach (RBA) for Grace Bay B.V. is designed to meet the regulatory requirements of the Curacao Gaming Control Board (GCB) 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.

3.4.1. 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.

3.4.2. 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.

3.4.3. Customer Risk Assessment

Grace Bay B.V. performs comprehensive customer risk assessments to identify and manage potential AML Crypto 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.

3.4.4. 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.

3.4.5. 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.

3.4.6. Geographical Risk and Jurisdictional Exposure

Grace Bay's global operations expose it to varying levels of AML Crypto 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.

3.4.7. 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.

3.4.8. 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.

3.4.9. 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.

3.4.10. 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.

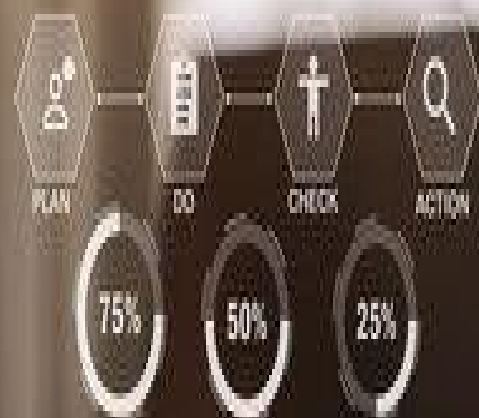
Transaction Monitoring: Real-time monitoring systems detect suspicious transactions, including significant deviations from normal transaction patterns, high-volume crypto-to-fiat conversions, and irregular deposit/withdrawal activities.

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.

4-Customer Due Diligence



4. Customer Due Diligence (CDD)

The Customer Due Diligence (CDD) outlines the procedures and requirements for Grace Bay B.V. in relation to Crypto (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.

4.1. 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 Control Board and international AML standards.

4.2. 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.

4.3. CDD Procedures

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

4.3.1. Identification and Verification

Individual Customers:

- Collect and verify the customer's full name, date of birth, residential address, and identification documents (passport, driver's license, or national ID).
- Verify the customer's identity using reliable third-party verification systems and databases.
- 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):

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

4.3.2. Customer Risk Profiling

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

- Geographical Risk: Customers from FATF high-risk jurisdictions, such as countries on the FATF's grey list, are considered high-risk.
- Transaction Patterns: Sudden large deposits, frequent cryptocurrency transactions, or withdrawals exceeding thresholds will be flagged for further scrutiny.

- Source of Funds: Determine whether the customer’s source of funds (crypto or fiat) is legitimate and consistent with their profile.
- 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.

4.3.3. Ongoing Monitoring

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

- Transaction Monitoring: Regularly review transaction patterns and the customer’s deposit and withdrawal behavior.
- 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.
- 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.

4.4. 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:

- Politically Exposed Persons (PEPs): Identifying and assessing any customers with political influence or who hold a public office.
- High-Risk Jurisdictions: Customers from countries with high levels of corruption or inadequate AML controls.
- 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:

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

4.5. 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:

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

4.6 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.

4.7. Suspicious Activity Reporting (SAR)

All staff involved in customer transactions are trained to detect and report suspicious activities. Indicators of suspicious activity may include:

- Unexplained large deposits or withdrawals.
- Frequent or unusual cryptocurrency exchanges.
- Customers attempting to circumvent transaction limits.
- Multiple accounts controlled by the same customer.
- Unverified third-party payments.

A person in a dark suit is seated at a desk, working on a laptop. The laptop screen displays a dashboard with the text 'KYC YOUR CUSTOMER' and a circular graphic. In the foreground, there is a spiral-bound notebook with a bar chart and a stack of papers. The background is dark and out of focus.

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

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

5.1 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 Control Board 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.

5.1.1. 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.

Initial Data Collection:

1. **Basic Information:** During registration, all customers must provide:
 - a) Full legal name
 - b) Date of birth (confirming they are of legal gambling age, 18+)
 - c) Nationality
 - d) Residential address
 - e) Contact information (email, phone number)
 - f) Unique ID documentation (passport, national ID, or driver's license)
2. **Proof of Identity:** Use a reliable document verification process to confirm the customer's identity via the upload of scanned ID documents.
3. **Proof of Address:** Customers are required to submit valid proof of address (utility bill, bank statement, government-issued letter) within the last 3 months.

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.

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.

5.1.2. 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).

5.1.3 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.

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.

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.

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.

5.2. In-House Sanctions Screening System

Grace Bay B.V In-House Sanctions Screening System, which covers all Crypto AML regulations required by the Curacao Gaming Control Board (GCB) and global Crypto 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.

5.2.1 Objectives of Sanction Screening System

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

5.2.2 Key Components of the In-House Sanctions Screening System

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.

5.2.3. 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.

5.2.4. 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.

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.

5.2.5. 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. 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.

5.2.6. 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 Control Board or international regulators) are notified, and the customer's account is immediately frozen pending further action.

5.3 In-House Transactions Monitoring System

Grace Bay B.V. has developed an In-House Transactions Monitoring System that complies with the Crypto AML regulations of the Curacao Gaming Control Board 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.

5.3.1. Key Features of the Transactions Monitoring System

The system is designed to monitor all types of transactions, particularly focusing on 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.

Deposit Monitoring

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

- a) **Name Mismatch Alerts:** If a player deposits funds under a different name from the registered account holder, an alert is generated.
- b) **Deposit Form Blank or Incomplete (Bank Transfers):** Any blank or incomplete bank transfer forms are flagged for review.
- c) **Incorrect Deposit Amount:** Deposits made with incorrect or unusual amounts (for both bank and crypto payments) are flagged for further investigation.
- d) **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.
- e) **Excessive Deposit Amounts:** Deposits significantly above the player's typical range trigger high-risk alerts, especially if they exceed standard daily limits.

Withdrawal Monitoring

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

- a) **Withdrawal to Different Accounts:** If the withdrawal is requested to an account not registered with the player, this triggers an immediate alert.
- b) **Mismatch in Withdrawal Method:** Withdrawals requested via a method different from the one used for deposits trigger an alarm, ensuring consistency in payment methods.
- c) **Excessive Withdrawals Relative to Deposits:** Withdrawals disproportionate to the amount deposited, particularly when there's little or no gameplay, will flag for AML investigation.
- d) **Withdrawal to Different Names:** Any withdrawals made to a name other than the registered account holder are flagged.
- e) **High-Value Withdrawals:** Withdrawals that exceed the player's average amount, especially those close to or above the set limits, trigger alerts.

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.

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.

5.3.2. 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.

5.3.3. 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.



6- Lines of Reporting & Record Keeping

6. Lines of Reporting & Record Keeping

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

6.1. 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 Crypto AML regulations of the Curacao Gaming Control Board (GCB) and international standards.

6.1.2 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 relevant authorities and law enforcement. All AML Staff will ensure that reports are compiled accurately, with all supporting documents, before submission to the GCB or international authorities as required.

6.1.2 Senior Management:

All AML Staff ensure 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.

6.1.3 External Authorities:

If suspicious transactions or activities are confirmed, the AML team 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

6.2 Record Keeping

To ensure compliance with Curacao Gaming Control Board 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:

6.2.1. 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.

6.2.2 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.

6.2.3 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.

6.2.4 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.

6.2.5 Communication Records:

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

6.2.6 Employee Training Records:

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

6.2.7. 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.

6.2.8. 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.



The image is a conceptual illustration for training and awareness. It features a large, glowing blue circular screen in the center, displaying a silhouette of a person holding a laptop. The screen is surrounded by various digital elements: a globe, a line graph, a bar chart, and a large letter 'C'. Below the screen, a person stands with their back to the viewer, facing the screen. In the foreground, a group of people are seated at desks, also facing the screen. The entire scene is set against a background of soft, white clouds and a warm, orange glow on the right side.

7- Training and Awareness

7. Training and Awareness

To ensure full compliance with Crypto Anti-Money Laundering (AML) regulations under the Curacao Gaming Control Board (GCB) 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.

7.1. General Training Requirements

Grace Bay B.V. requires all employees, regardless of their position, to undergo Crypto 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.

7.2 Training Frequency:

Initial Training: Provided to all new employees during onboarding, ensuring they understand the company's Crypto 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 Crypto 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 Crypto AML regulations or company operations.

7.3. 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 Crypto AML Training 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 Crypto AML compliance.

