

LOTOSTORM B.V. (163910)

Abraham Mendez Chumaceiro Boulevard 03, Curacao



AML/CTF/CPF Policy

February 2025

Approved by the Board of Directors

Two blue ink signatures, one above the other, representing the approval of the Board of Directors.

Table of Contents

- 1. Policy Statement**
- 2. Responsibilities of the Management**
- 3. iGaming Landscape**
- 4. Money Laundering**
- 5. Terrorism Financing**
- 6. Proliferation Financing**
- 7. Sanctions**
- 8. Risk-Based Approach: Money Laundering, Terrorism Financing, Proliferation Financing**
 - 8.1. iGaming Risk Factors**
 - 8.2. Technological Development Risk Assessment**
- 9. Customer Due Diligence**
 - 9.1. CDD Measures in Detail**
 - 9.2. Player Identification & Verification**
 - 9.3. Understanding the Business Relationship**
 - 9.4. Ongoing Monitoring**
 - 9.5. Simplified & Enhanced Due Diligence**
 - 9.6. Timing of CDD Measures**
 - 9.7. Existing Clients**
 - 9.8. Termination of Relationships**
 - 9.9. Third-Parties Usage for CDD**
- 10. Suspicious Activity Reporting**
- 11. Compliance Officer**
- 12. Employee Training**
- 13. Record Keeping**
- 14. Independent Audit**
- 15. Annexes**
 - Annex 1. Definitions**
 - Annex 2. Abbreviations**

1. Policy Statement

LOTOSTORM B.V. (163910) has developed an Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing Policy (AML/CTF/CPF Policy) to actively prevent financial crimes such as money laundering and terrorism financing. This policy is structured to align with both domestic and international AML/CTF/CPF standards and ensures strict adherence to relevant regulatory requirements. It establishes a comprehensive risk management framework covering various aspects, including customer engagement, product and service offerings, payment channels, geographic areas of operation, and service delivery methods.

The Board of Directors (BoD) of LOTOSTORM B.V. holds the responsibility for approving, enforcing, and overseeing the AML/CTF/CPF Policy. This policy undergoes an annual review and may be revised as necessary to incorporate significant regulatory or operational updates. Additionally, a designated officer may recommend immediate amendments in response to findings from internal and external AML audits, taking into account potential risks and implications.

This AML/CTF/CPF Policy is structured in accordance with key international and Curaçao regulatory frameworks. LOTOSTORM B.V. strictly adheres to the Regulations for Combating Money Laundering, Terrorism Financing, and the Proliferation of Weapons of Mass Destruction (ML/FT/FP) as these regulations are a fundamental component of iGaming licensing requirements within the Curaçao jurisdiction and are at the core of the Company's operations:

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

Through these regulations, the Curaçao Gaming Control Board (GCB) provides a structured framework to guide casinos and gambling operators in ensuring compliance with laws and decrees related to money laundering, terrorism financing, and proliferation financing. This framework serves as the core of LOTOSTORM B.V. development and implementation of internal policies and procedures to mitigate financial crime risks.

The key regulatory provisions LOTOSTORM B.V. complies with include, but are not limited to:

- The National Ordinance on Identification of Clients When Rendering Services (N.G. 2017, no. 92);

- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
- Ministerial Decree (dated November 11, 2015) outlining indicators under Article 10 of the National Ordinance on Reporting Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree on the Enforcement of the Kingdom Sanction Law (N.G. 2017, no. 2);
- National Decree (dated July 10, 2015) implementing UN Security Council Resolutions regarding Al-Qaeda, the Taliban, ISIL, ANF, and other designated individuals and organizations (N.G. 2015, no. 29);
- National Decree (dated July 10, 2015) implementing Article 2 of the Sanctions National Ordinance concerning Libya (Sanctions Ordinance Libya) (N.G. 2015, no. 28);
- National Decree (dated July 10, 2015) implementing Article 2 of the Sanctions National Ordinance concerning UN Security Council Resolutions 1695 (2006), 1718 (2006), 2087 (2013), and 2094 (2013) (Sanctions National Ordinance Extension of Validity Sanction Decrees 2018) (N.G. 2018, no. 34);
- The Penal Code (Code of Criminal Law) (N.G. 2011, no. 48).

These laws and regulations, along with any supplementary measures established under the NOIS, NORUT, the Sanctions National Ordinance, and the Kingdom Sanction Law, form the primary legal framework that governs the Curaçao gaming industry in its efforts to prevent money laundering, terrorism financing, and the proliferation of weapons of mass destruction.

In addition to local regulations, this policy incorporates global best practices and follows guidelines from recognized international organizations, including but not limited to the Financial Action Task Force (FATF) Recommendations, the European Union's 4th, 5th, and 6th Anti-Money Laundering Directives (AMLDs), and the Wolfsberg Principles.

Ultimately, the AML/CTF/CPF Policy of LOTOSTORM B.V. (163910) is designed to meet the compliance requirements set by Curaçao's AML/CTF/CPF supervisory authority, the Curaçao Gaming Control Board. All company directors, officers, employees, and third-party auditors engaged in compliance assessments are required to adhere to and uphold the principles outlined in this policy.

2. Responsibilities of the Management

The role of senior management within LOTOSTORM B.V. (163910) is crucial in assessing and mitigating risks associated with Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF). To ensure effective oversight, the Board of Directors (BoD) mandates that the appointed

AML/CTF/CPF Officer provides regular reports on significant changes or emerging issues in the control framework. Additionally, this officer is responsible for submitting an annual assessment evaluating the efficacy of the company's safeguards against money laundering, terrorist financing, and proliferation financing risks.

Senior management is also accountable for reviewing policies and procedures annually to ensure they remain effective and up to date. These reviews are guided by monthly risk assessments, which help identify any vulnerabilities within internal controls and risk management systems. In the event of identified deficiencies, the AML/CTF/CPF Officer may recommend necessary modifications to the Board for approval, thereby enhancing the company's compliance framework.

In line with global regulatory standards, senior management oversees the development and execution of comprehensive employee training programs. These training sessions are designed to increase awareness of AML/CTF/CPF risks, equipping employees—especially those in key positions—with the necessary knowledge to identify and respond to suspicious activities effectively.

Furthermore, senior management is responsible for ensuring that the company's internal control mechanisms remain robust. This includes maintaining clear role segregation, defined authorization protocols, continuous monitoring, and proper documentation. To reinforce compliance and optimize the effectiveness of the AML/CTF/CPF program, regular independent audits and assessments are conducted to offer an unbiased review and pinpoint potential areas for improvement.

3. iGaming Landscape

LOTOSTORM B.V. (163910) is a legally registered entity in Curaçao that owns and operates the website <https://clickpari.com>. The company holds an online gaming license issued by the Curaçao Gaming Control Board, specifically OGL/2024/303/0300, and complies with all licensing regulations and regional restrictions established by the Curaçao regulatory authorities. These regulations strictly prohibit remote gaming licensees from providing services in certain jurisdictions, including the United States, Australia, the Dutch West Indies (Aruba, Bonaire), Curaçao, France, Germany, the United Kingdom, Belize, and the Netherlands. As a result, the company operates only in legally authorized markets and refrains from targeting customers in regions where online gambling is prohibited.

Like other e-gaming and betting operators, LOTOSTORM B.V. is exposed to various money laundering risks, including identity theft, fraudulent activities, structuring, layering, and the potential for collusion between employees, customers, or third-party payment providers to bypass internal security controls.

4. Money Laundering

Money laundering is a key component of financially motivated crime, often involving cross-border operations. It is linked to various illegal activities, including tax evasion, fraud, corruption, sanctions violations, drug trafficking, illegal arms trade, extortion, and kidnapping. The primary objective of money laundering is to conceal the illicit origins of proceeds derived from criminal activities by obscuring their source, identity, and final destination.

The Three Stages of Money Laundering

1. **Placement** – This is the initial stage, where illicit funds are introduced into the financial system. This is done through bank deposits, purchasing high-value assets, or conducting various financial transactions. The goal at this phase is to start integrating illegal funds into the legitimate economy.
2. **Layering** – In this phase, the money is moved through multiple complex transactions to further obscure its origins. Techniques include transferring funds across numerous accounts, converting funds into different currencies, or investing in various financial instruments. This process is intended to eliminate traceability, making it difficult to link the funds back to criminal activities.
3. **Integration** – The final stage involves reintroducing the laundered funds into the legal economy. This may be done through purchasing luxury assets, investing in cash-intensive businesses, or engaging in other seemingly legitimate financial transactions. At this point, the money appears clean, making it significantly harder to trace back to its illicit source.

Money laundering can occur at different stages of financial transactions, and online gambling platforms are particularly vulnerable to being exploited for this purpose. This underscores the importance of preventing anonymous transactions and identifying suspicious activities.

Terrorist Financing and Its Connection to Money Laundering

Terrorist financing refers to the movement of funds used to support terrorist activities. Unlike money laundering, these funds may originate from legitimate sources but are transferred through financial systems in a way that resembles laundering techniques. Prepaid cards, for example, are frequently used to fund terrorist operations by purchasing materials for attacks. To combat such risks, LOTOSTORM B.V. (163910) ensures that employees receive ongoing training on emerging trends and evolving threats related to terrorist financing.

Risk Management and Compliance Measures

To mitigate money laundering risks, LOTOSTORM B.V. (163910) adopts a proactive approach by detecting, assessing, and addressing potential threats. Key compliance strategies include:

- **Fraud and Identity Verification** – Implementing customer due diligence (CDD) processes, including document verification, age validation, and location checks.
- **Monitoring Multiple Accounts and High-Value Transactions** – Identifying unusual account activity, including the use of multiple accounts or frequent large transactions.
- **Detecting Illicit Fund Deposits** – Screening for suspicious deposits originating from illicit activities and preventing the platform from being used as a temporary holding space for such funds.
- **Player-to-Player Transfers** – Monitoring for potential misuse of the platform to transfer illicit funds between users or enable fraudulent cash-out activities.

This list is not exhaustive, as new risks may emerge over time. To ensure robust compliance, LOTOSTORM B.V. (163910) conducts regular risk assessments tailored to evolving threats and provides ongoing training to employees to reinforce its Anti-Money Laundering (AML) compliance framework.

5. Terrorism Financing

Terrorist financing refers to the funding of terrorist activities, utilizing both legitimate and illicit financial sources. These funds are critical for carrying out operations ranging from small-scale activities to large-scale attacks.

Sources of Terrorist Financing

The sources of financing can be broadly divided into legal and illegal categories:

- **Legal Sources** – Terrorists may exploit legitimate businesses, charitable donations, and legal financial transactions to funnel funds. In some cases, charitable organizations and commercial enterprises are misused as conduits to disguise and redirect money.
- **Illegal Sources** – Criminal activities such as fraud, smuggling, drug trafficking, extortion, and money laundering are commonly used to generate funds while obscuring their origins.

Methods of Fund Transfers

Terrorist financing networks use various channels to move funds:

- Formal Financial Channels – Traditional banking systems and financial institutions are sometimes exploited through sophisticated techniques like layering and structuring, which help avoid detection by breaking transactions into smaller, less suspicious amounts.
- Informal Transfer Systems – Alternative financial networks such as the hawala system operate outside regulated financial institutions, making it difficult for authorities to trace transactions.

Indicators of Terrorist Financing

Certain transaction patterns may indicate potential terrorist financing, including:

- Unusual financial activity that deviates from typical business or personal behavior.
- Frequent or high-value transactions involving high-risk regions known for terrorist activities.
- Transactions associated with individuals or entities linked to terrorism, including those flagged on international watchlists.
- Large cash deposits, high-risk industry transactions, or financial activities that seem structured to avoid scrutiny.

Regulatory Compliance and Countermeasures

To combat terrorist financing, LOTOSTORM B.V. (163910) implements a comprehensive AML compliance program that includes:

- Customer Due Diligence (CDD) – Verifying customer identities, sources of funds, and potential risks.
- Transaction Monitoring – Analyzing financial transactions for suspicious patterns.
- Reporting Suspicious Activities – Notifying relevant authorities of any potential terrorist financing indicators.

The company also adheres to multiple sanctions lists and regulatory directives, including:

- Sanctions National Ordinance (SNO, N.G. 2014, no. 55)
- Kingdom Sanction Act (N.G. 2016, no. 54)
- Curaçao Gaming Control Board (GCB) regulatory announcements
- Office of Foreign Assets Control (OFAC) watchlists
- United Nations Security Council (UNSC) sanctions lists
- European Union (EU) anti-terrorism financial regulations
- U.S. List of Foreign Terrorist Organizations

These sanctions and regulatory measures help ensure that the company does not inadvertently facilitate financial transactions that may support terrorism.

Global Framework for Counter-Terrorism Financing

- Financial Action Task Force (FATF) – Establishes international standards for detecting and reporting suspicious financial activity related to money laundering and terrorist financing.
- Office of Foreign Assets Control (OFAC) – Enforces U.S. economic sanctions and maintains the Specially Designated Nationals (SDN) list, which includes individuals and entities associated with terrorism.
- European Union (EU) – Enforces regulatory frameworks designed to prevent the exploitation of financial systems for terrorist activities, requiring member states to implement strong AML measures.
- United Nations (UN) – Imposes international sanctions and maintains watchlists of individuals and organizations involved in terrorism, supporting global efforts to restrict financial access for terrorist groups.

By implementing strict compliance policies and adhering to international regulatory frameworks, LOTOSTORM B.V. (163910) strengthens its ability to detect, prevent, and report terrorist financing activities, ensuring a secure and legally compliant operational environment.

6. Proliferation Financing

Proliferation financing involves the funding, support, or facilitation of activities related to the development, acquisition, and distribution of weapons of mass destruction (WMDs) and their delivery systems. This type of financial activity represents a serious global security threat and is strictly prohibited under both international and Curaçao regulations. As a licensed iGaming operator, LOTOSTORM B.V. (163910) is committed to identifying and mitigating proliferation financing risks as part of its broader Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) compliance framework.

Compliance with Curaçao iGaming Regulations

The Curaçao Gaming Control Board (GCB) has implemented strict regulatory requirements to address proliferation financing risks, ensuring alignment with global compliance standards. These requirements mandate that all licensed operators, including LOTOSTORM B.V. (163910), take active measures to detect, mitigate, and report potential proliferation financing threats.

Key Compliance Measures

Risk Assessment

LOTOSTORM B.V. (163910) conducts regular risk assessments to evaluate vulnerabilities within its operations related to proliferation financing. These assessments focus on:

- Identifying customers from high-risk jurisdictions known for weak proliferation controls.
- Detecting transactions linked to goods, services, or entities associated with WMD proliferation networks.
- Analyzing financial patterns that resemble known proliferation financing tactics.

Enhanced Customer Due Diligence (CDD)

To strengthen its compliance framework, LOTOSTORM B.V. (163910) implements enhanced CDD procedures for high-risk customers. This includes:

- Screening customers against global sanctions lists, such as those issued by the United Nations Security Council (UNSC), the Financial Action Task Force (FATF), and the European Union (EU).
- Investigating unusual transactions that deviate from expected customer behavior.
- Monitoring affiliations with organizations flagged for involvement in proliferation-related activities.

Transaction Monitoring and Reporting

The company employs advanced transaction monitoring systems to detect suspicious financial activity. These systems:

- Analyze transaction behavior to identify potential proliferation financing indicators.
- Flag high-risk financial movements for further review.
- Ensure suspicious activity reports (SARs) are promptly submitted to the Curaçao Financial Intelligence Unit (FIU).

Sanctions Screening and Compliance

LOTOSTORM B.V. (163910) adheres to Curaçao and international sanctions regulations by:

- Blocking transactions involving individuals, entities, or jurisdictions subject to WMD-related sanctions.
- Screening all financial transactions and business relationships against regularly updated sanctions lists, including those under the Kingdom Sanction Act and United Nations Security Council Resolutions.

- Maintaining comprehensive records of sanctions screenings and compliance actions for regulatory audits.

Training and Awareness

All employees undergo specialized training on proliferation financing risks, equipping them to:

- Recognize red flags associated with proliferation financing.
- Respond appropriately to potential threats.
- Stay up-to-date with Curaçao's evolving regulatory framework.

Collaboration with Authorities

LOTOSTORM B.V. (163910) actively cooperates with:

- The Curaçao Gaming Control Board (GCB)
- The Financial Intelligence Unit (FIU)
- Other relevant regulatory bodies

This collaboration includes supporting investigations, timely reporting of suspicious activities, and participating in industry-wide initiatives to combat proliferation financing within the iGaming sector.

Commitment to Global Security

LOTOSTORM B.V. (163910) remains dedicated to preventing its platform from being exploited for proliferation financing activities. By complying with Curaçao's latest iGaming regulatory requirements and international compliance frameworks, the company reinforces its commitment to maintaining a secure, transparent, and legally compliant gaming environment. These efforts contribute to the global fight against financial networks supporting WMD development and distribution, ensuring the integrity of the financial system.

7. Sanctions

LOTOSTORM B.V. (163910) is committed to strict compliance with international sanctions and regulatory requirements as part of its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) policy. To uphold these obligations, the company implements comprehensive compliance procedures, ensuring adherence to all sanctions imposed by national and international regulatory bodies. This involves conducting extensive due diligence on all clients and transactions to prevent any engagement with sanctioned individuals, entities, or jurisdictions.

Transaction Monitoring and Reporting

A core component of the company's AML/CTF/CPF policy is the continuous monitoring of transactions to detect potential sanctions breaches. Any suspicious activity or irregular transactions are immediately flagged and reported to the relevant authorities. To reinforce its commitment to compliance, the company provides ongoing training programs for its employees, ensuring they stay informed about current sanctions regulations and enforcement measures.

Automated Sanctions Screening and Compliance Actions

LOTOSTORM B.V. (163910) ensures that all client interactions and transactions are thoroughly screened against the most recent sanctions lists. Automated compliance systems perform real-time verification checks, and the company's internal database is consistently updated with the latest sanctions information. If a sanctions match or suspicious activity is detected, it is promptly reported to the relevant authorities. The company takes decisive actions, such as freezing accounts or blocking transactions, to mitigate compliance risks and prevent any violations.

Regular Policy Reviews and Adherence to Evolving Regulations

The company's sanctions compliance framework is subject to frequent reviews and updates to ensure alignment with changing regulatory requirements. The compliance process includes active monitoring of the following sanctions lists:

- Sanctions National Ordinance (SNO, N.G. 2014, no. 55)
- Kingdom Sanction Act (N.G. 2016, no. 54)
- Curaçao Gaming Control Board (GCB) announcements
- European Union (EU) sanctions
- United Kingdom Office of Financial Sanctions Implementation (UK OFSI) sanctions
- United Nations Security Council (UNSC) Consolidated List
- U.S. List of Foreign Terrorist Organizations
- Office of Foreign Assets Control (OFAC) sanctions

Preventing Sanctions Evasion and Strengthening Compliance Measures

The company's due diligence efforts extend to detecting indirect or concealed attempts to circumvent sanctions. If any evasion tactics are identified, they are immediately reported to the appropriate authorities. To address such risks, the company takes corrective actions, including transaction suspensions, account reviews, and enhanced monitoring.

To further strengthen compliance, regular audits are conducted, and staff training programs are continuously updated. This proactive approach ensures that LOTOSTORM B.V. (163910) remains fully compliant with regulatory requirements and best practices in preventing sanctions evasion and financial crime.

8. Risk-Based Approach: Money Laundering, Terrorism Financing, Proliferation Financing

A key component of LOTOSTORM B.V. (163910)'s compliance strategy is its comprehensive risk assessment, which follows a risk-based approach (RBA). This process entails a thorough evaluation of risks associated with customers, products, services, and geographic locations. The company conducts regular assessments to proactively identify potential vulnerabilities and implement effective mitigation strategies.

Risk Mitigation Strategies

Once potential risks are identified, LOTOSTORM B.V. (163910) applies tailored mitigation measures based on the level of risk exposure. These strategies include:

- Enhanced Due Diligence (EDD) – Conducting in-depth investigations on high-risk customers and transactions, including:
 - Collecting additional details on source of funds.
 - Verifying beneficial ownership structures.
- Sophisticated Transaction Monitoring – Utilizing automated systems to detect suspicious financial activities by:
 - Setting alert thresholds for unusual transaction patterns.
 - Identifying behaviors consistent with money laundering or terrorist financing.
- Strict Customer Verification Procedures – Applying robust identity verification measures for high-risk individuals, including:
 - Authentication through trusted data sources.
 - Ongoing monitoring of flagged individuals to detect emerging risks.

Ongoing Monitoring and Policy Updates

To ensure continuous compliance, LOTOSTORM B.V. (163910) conducts regular reviews of transaction data to:

- Detect emerging suspicious activities.
- Update customer risk profiles based on newly obtained information.
- Revise AML/CTF/CPF policies and procedures to reflect evolving regulatory requirements and risk trends.

Accurate Reporting and Record-Keeping

Precise reporting and record management are essential to the company's risk-based compliance program. LOTOSTORM B.V. (163910) ensures that:

- Suspicious transactions are promptly reported to the appropriate authorities.
- Detailed records of customer identification, financial transactions, and risk assessments are maintained for the legally mandated period.
- Records remain accessible for regulatory audits and inspections.

By implementing these proactive measures, LOTOSTORM B.V. (163910) upholds its commitment to maintaining a secure, transparent, and compliant operational environment in accordance with AML/CTF/CPF regulatory standards.

8.1. iGaming Risk Factors

Customer Risks:

Customer risk refers to the potential money laundering (ML) and terrorism financing (TF) risks associated with engaging in business relationships with specific individuals. The process of LOTOSTORM B.V. risk assessment involves evaluating the customer's profile, financial activities, and sources of wealth.

Certain customer categories may indicate a higher risk level, including:

- Customers with multiple income sources – Higher complexity in financial transactions can make it difficult to verify the legitimacy of funds.
- Individuals with irregular income streams – Fluctuating or unpredictable financial patterns may suggest an increased risk of illicit activity.
- Politically Exposed Persons (PEPs) – Due to their influence and access to public funds, PEPs pose a higher corruption and financial crime risk.
- High-spending individuals – Large expenditures may indicate potential proceeds from illegal activities.
- Disproportionate spenders – Spending that appears inconsistent with a customer's known income or assets could signal suspicious financial behavior.
- Customers utilizing multiple accounts – This tactic can obscure a player's gambling activity and prevent accurate tracking of transaction patterns.

Transaction Thresholds and Risk-Based Approach

To mitigate ML/TF risks, LOTOSTORM B.V. (163910) established transaction thresholds that represent typical financial behavior for their customer base, for instance:

- Low-Risk Customers – Individuals with a single, verifiable, and regular source of income pose less risk.
- Higher-Risk Customers – Players with multiple income sources or irregular financial patterns require enhanced monitoring and additional due diligence.

Product, Service & Transaction Risks:

Certain products, services, and transaction methods pose a higher risk of being exploited for money laundering (ML) and terrorist financing (TF). Criminals often target vulnerable financial and gaming mechanisms, particularly those that allow them to manipulate game outcomes individually or in collaboration with others. Additionally, certain payment methods that present heightened ML/TF risks should be considered high-risk factors.

Key High-Risk Products, Services, and Transactions

- Proceeds from criminal activities – Funds may originate from illegal activities, including:
 - Credit/debit card fraud
 - Drug trafficking
 - Theft from an employer
- Anonymous payment methods – These present an elevated risk due to a lack of traceability. Examples include:
 - Prepaid cards
 - Virtual assets (cryptocurrencies, digital tokens, etc.)
- Accounts misuse – Player accounts should be used solely for gambling purposes and not as deposit/withdrawal conduits with little or no playing history.
- Peer-to-peer gaming – Enables players to transfer funds among themselves, increasing the risk of illicit financial activity.
- Third-party financial instruments – Includes customers using:
 - Bank accounts or payment cards registered under someone else's name.
- Funds transferred between different gaming accounts to disguise illicit transactions.
- Financial services linked to gambling – Certain financial services present increased risks, including:
 - Credit and marker issuance
 - Currency exchange
- Multiple gaming accounts or wallets – Online operators may manage multiple websites, which allows criminals to:
 - Open several accounts under different identities.
 - Move funds between platforms to complicate tracking.
- Changing financial institution details – Frequent modifications to linked bank accounts or payment methods used to fund accounts may indicate attempts to evade detection.
- Identity fraud – Criminals may use:
 - Stolen financial account details to gamble online.
 - Fraudulently opened bank accounts to conduct illicit transactions.
- Cash-funded prepaid cards – Carry similar risks to direct cash transactions, as they provide a layer of anonymity.
- Multi-operator gaming networks – Games shared across multiple gaming platforms (e.g., online poker) allow cross-border financial movements, increasing ML/TF risks.
- Electronic wallets (e-wallets) – Certain e-wallets present risks due to:

- Operating in non-reputable jurisdictions.
- Masking transactions—Financial institution statements only show payments to the e-wallet, without detailing transactions. This can be exploited by customers attempting to obscure gambling activity.

LOTOSTORM B.V. (163910) identifies and documents all products, services, and payment methods that are considered high-risk. These risks are monitored and addressed through enhanced due diligence (EDD), transaction monitoring, and regulatory compliance measures to mitigate financial crime exposure within the gaming environment.

Geographical Risk:

Geographical risk refers to the potential money laundering (ML), terrorism financing (TF), and proliferation financing (PF) risks associated with the player's location and the origin of their financial resources. A player's nationality, country of residence, and place of birth are key factors in determining risk exposure, as some jurisdictions pose higher financial crime risks than others.

Countries are considered high-risk if they:

- Lack a robust AML/CFT framework.
- Have high levels of corruption.
- Are subject to international sanctions due to terrorism financing or involvement in the proliferation of weapons of mass destruction (WMDs).
- Are known to harbor terrorist organizations or provide financial support for terrorism.

Trusted Sources for Identifying High-Risk Jurisdictions

To assess geographical risks, LOTOSTORM B.V. (163910) refers to reputable international regulatory bodies and recognized independent organizations, including:

- Financial Action Task Force (FATF) Reports:
- High-Risk Jurisdictions Subject to a Call for Action.
- Jurisdictions Under Increased Monitoring.
- Caribbean Financial Action Task Force (CFATF) Public Statements.
- U.S. Department of State – International Narcotics Control Strategy Report (INCSR):
- Identifies Jurisdictions of Concern and Primary Concern.
- European Commission's List of High-Risk Third Countries:
- Highlights jurisdictions with strategic deficiencies in AML/CFT regulations.
- Office of Foreign Assets Control (OFAC) Sanctions List:
- Includes countries subject to U.S. financial restrictions due to terrorism, proliferation activities, or other national security threats.

- Reports from Credible Global Organizations:
- Countries identified as sponsors of terrorism or as hosting terrorist organizations.
- Transparency International's Corruption Perceptions Index (CPI), which ranks countries based on their levels of corruption.

Risk Categorization and Policy Implementation

To effectively manage geographical risk, LOTOSTORM B.V. (163910) maintains a structured risk classification system, categorizing countries into high-risk and low-risk groups. This classification is used to:

- Apply enhanced due diligence (EDD) measures for players from high-risk jurisdictions.
- Restrict transactions involving sanctioned countries.
- Continuously update monitoring systems to reflect evolving global risk assessments.

By utilizing data-driven risk assessments, LOTOSTORM B.V. (163910) ensures compliance with AML/CTF/CPF regulations, preventing financial crime while maintaining a secure and transparent gaming environment.

Distribution Channels Risk:

Key Risk Factors in Distribution Channels

1. Anonymity-Driven Channels – Channels that allow anonymous transactions or interactions pose a greater risk of ML/TF unless adequate measures are implemented to mitigate such risks.

Risk Mitigation Strategies

To address and manage risks associated with distribution channels, LOTOSTORM B.V. (163910):

- Implements enhanced verification controls for anonymous transactions.
- Utilizes technological solutions, such as biometric authentication, identity verification, to prevent fraud in non-face-to-face interactions.

By enforcing robust monitoring and secure authentication measures, LOTOSTORM B.V. (163910) reduces the risks associated with high-risk distribution channels while maintaining regulatory compliance and customer security.

8.2. Technological Developments Risk Assessment

LOTOSTORM B.V. (163910) is committed to preventing the misuse of technological advancements for money laundering (ML) and terrorist financing (TF). To achieve this, the company maintains robust procedures and controls to identify and mitigate risks associated with emerging technologies, business practices, and delivery mechanisms.

Risk Identification and Assessment

The company conducts a comprehensive risk assessment whenever:

- A new product or service is introduced.
- A new business practice is implemented.
- A new method of delivering services becomes available.
- A new or evolving technology is integrated into existing or new products.

Before launching any new innovation, a thorough risk evaluation is conducted to assess whether it introduces vulnerabilities that could be exploited for financial crimes. All risk assessments are documented to ensure compliance with regulatory requirements.

Risk Mitigation Measures

If risks are identified, LOTOSTORM B.V. (163910) takes proactive measures to minimize potential threats. This includes:

- Implementing enhanced security controls to prevent misuse.
- Strengthening monitoring systems to detect anomalies in financial transactions.
- Updating AML/CTF compliance policies to align with new technological risks.

By continuously evaluating and adapting to technological changes, LOTOSTORM B.V. (163910) ensures a secure, compliant, and resilient operational environment against financial crime threats.

9. Customer Due Diligence

LOTOSTORM B.V. (163910) strictly adheres to regulatory requirements that prohibit anonymous or fraudulent accounts. As part of its AML/CTF/CPF compliance framework, the company implements rigorous identity verification procedures to establish and understand business relationships with its players. These measures play a critical role in detecting and preventing money laundering, terrorist financing, and proliferation financing. A comprehensive CDD program allows the company to assess potential risks and ensure compliance with regulatory expectations. Any suspicious activities are promptly reported to the Financial Intelligence Unit (FIU) and, if necessary, escalated to the Public Prosecutor's Office.

9.1 CDD Measures in Detail

Player Identification and Verification

As part of its CDD process, LOTOSTORM B.V. (163910) applies the following measures:

- Verifying player identities using official, independent, and reliable documentation or data sources.
- Determining and confirming the ultimate beneficial owner (UBO) for legal entities to understand ownership and control structures.
- Assessing the purpose and intended nature of the business relationship.
- Ongoing due diligence and transaction monitoring, ensuring consistency with expected customer behavior and risk profiles. This includes verification of the source of funds when necessary.

Confidentiality of Reports

To prevent tipping off customers, the Company's staff are strictly prohibited from disclosing when a suspicious activity report (SAR) is submitted to the FIU. If CDD measures could potentially alert the player to an ongoing investigation, the Company may bypass the process and immediately file a report with the FIU.

9.2. Player Identification & Verification

Required Identification Information:

To verify a player's identity, the following details are collected:

- Full legal name
- Permanent residential address
- Date of birth
- Place of birth
- Nationality
- Official identification number

For lower-risk customers, only basic identification details are required. However, for higher-risk individuals, additional verification measures are applied to mitigate potential money laundering and terrorist financing risks.

Risk Assessment and Verification Process

- Initial risk ratings are assigned based on collected player information and are continuously updated as more data becomes available.
- Verification of identity is conducted through:
 - Government-issued photo ID (passport, national ID card, driver's license).
 - Supporting documents (e.g., utility bill or bank statement, issued within the last six months) to confirm residential address.
- Verification of address via official correspondence (e.g., letters, emails, phone confirmations).
- Biometric verification, database cross-referencing, IP tracking, and validation of funding methods.

If the collected information is insufficient, additional verification steps may be required, such as:

- Requesting a live selfie with the ID document.
- Confirming the first deposit through a regulated financial institution.

By implementing robust CDD measures, LOTOSTORM B.V. (163910) ensures a secure and compliant gaming environment, reducing exposure to financial crime risks while maintaining strict regulatory compliance.

9.3. Understanding the Business Relationship

As part of its Customer Due Diligence (CDD) process, LOTOSTORM B.V. (163910) seeks to understand the purpose and nature of its business relationships with players. While the relationship's primary purpose—gambling activity—is generally clear, the company collects sufficient information to identify potentially unusual or suspicious activities.

For higher-risk clients, the company conducts enhanced due diligence (EDD), which includes:

- Detailed documentation of the source of wealth to verify the legitimacy of funds.
- Assessment of expected activity levels, ensuring they align with the player's financial profile.
- Cross-referencing independent data sources to validate provided information.

For lower and medium-risk players, a simplified verification process is applied:

- A basic declaration stating their employment or business details is required.
- Additional verification measures are conducted only if suspicious patterns arise.

By categorizing customers based on risk levels, LOTOSTORM B.V. (163910) ensures proportionate monitoring and due diligence, preventing financial crime while maintaining regulatory compliance.

9.4. Ongoing Monitoring

As part of its AML/CTF/CPF compliance framework, LOTOSTORM B.V. (163910) conducts continuous monitoring of player identities and transactions to detect and prevent money laundering, terrorist financing, and proliferation financing.

Key monitoring measures include:

- Regular updates and verification of player information, particularly for high-risk individuals.
- Transaction monitoring to identify unusual patterns or suspicious activity.
- Enhanced Due Diligence (EDD) for transactions meeting or exceeding NAF 4,000, including linked transactions that collectively surpass this threshold.
- Advanced monitoring systems that operate in real-time, analyzing transactions for potential red flags and ensuring immediate investigation and reporting to the Financial Intelligence Unit (FIU) when necessary.

By integrating automated risk detection with manual oversight, LOTOSTORM B.V. (163910) enhances its ability to identify and respond to suspicious financial activities, reinforcing its commitment to regulatory compliance and operational security.

9.5. Simplified & Enhanced Due Diligence

Simplified Due Diligence (SDD)

In cases where the risk of money laundering (ML) or terrorist financing (TF) is assessed to be low, LOTOSTORM B.V. (163910) may apply Simplified Customer Due Diligence (SDD) measures. These measures are tailored to reflect the reduced risk level while ensuring compliance with AML/CTF/CPF regulations.

Examples of Simplified CDD Measures

- Limited Data Collection – If a risk assessment confirms a low ML/TF risk, the Company may collect only the player's basic identity information, such as:
 - Full name
 - Date of birth
 - Permanent residential address

- Delayed Verification – In lower-risk scenarios, the verification of customer identity and beneficial ownership may be conducted after the business relationship has been established.
- Risk-Based Verification – The depth of verification may be adjusted depending on the assessed risk level:
- In low-risk cases, the Company may rely on alternative reputable data sources, even those without photographic identification.
- Minimal Personal Detail Verification – The company may choose to verify only essential identity details, provided there is sufficient assurance that the customer's identity is legitimate.
- Reduced Frequency of Customer Information Updates – Players in low-risk categories may be subject to less frequent identity verification updates.
- Lower Intensity of Transaction Monitoring – Transactions may be monitored less frequently or within a reasonable monetary threshold, reflecting the low risk associated with the business relationship.

Limitations of Simplified Due Diligence

- SDD cannot be applied in cases where ML/TF is suspected.
- Higher-risk scenarios always require standard or enhanced due diligence (EDD).

By applying SDD only in appropriate cases, LOTOSTORM B.V. (163910) ensures a risk-sensitive approach while maintaining regulatory compliance and financial security.

Enhanced Due Diligence (EDD)

LOTOSTORM B.V. (163910) follows a risk-based approach in its Customer Due Diligence (CDD) framework, ensuring that higher-risk customers are subject to Enhanced Due Diligence (EDD). This process involves more rigorous verification and monitoring measures, aligning with the specific risks identified. The company intensifies monitoring of business relationships to detect and assess unusual activities or suspicious transactions.

When Enhanced Due Diligence is Required

EDD is mandatory in cases where the risk of money laundering (ML) or terrorist financing (TF) is higher, including:

- Residents of high-risk geographic regions – Customers from jurisdictions with weak AML/CFT controls, high corruption levels, or international sanctions require additional scrutiny.

- Politically Exposed Persons (PEPs) – Due to their influence and access to public funds, PEPs pose an increased corruption and financial crime risk, necessitating enhanced identity verification and transaction monitoring.
- Products or transactions that facilitate anonymity – Transactions conducted using anonymous payment methods (e.g., prepaid cards, virtual assets) require stricter monitoring and verification.
- New products, business practices, or technologies – Any new delivery mechanisms or emerging financial technologies (such as cryptocurrency transactions or blockchain-based gaming services) must be assessed for potential financial crime risks before implementation.

The Enhanced Due Diligence (EDD) measures implemented by LOTOSTORM B.V. (163910) must be proportionate to the risks identified. These measures focus on increasing the level of scrutiny and monitoring business relationships to detect unusual or suspicious transactions.

Examples of EDD Measures

1. Collecting Additional Customer Information
 - Gathering occupation details, previous addresses, and data available through public records, online sources, and independent databases.
2. Understanding the Business Relationship
 - Requesting additional details about the intended nature of the relationship between the customer and the Company.
3. Verifying Source of Funds and Source of Wealth
 - Determining how the player's funds were acquired, which may include:
 - Personal savings
 - Employment income
 - Pension withdrawals
 - Sale of shares or dividend payouts
 - Proceeds from property sales
 - Gambling winnings
 - Inheritance or financial gifts
 - Legal settlements or compensation payments
4. Assessing the Purpose of Transactions
 - Obtaining explanations for planned or completed transactions, particularly those that appear unusual or inconsistent with customer behavior.
5. Senior Management Approval
 - Requiring senior management authorization to:

- Initiate or continue a business relationship with a high-risk customer.
6. Enhanced Transaction Monitoring
- Implementing continuous monitoring of the business relationship, with real-time alerts on high-risk transactions.
7. Ensuring Transactions Originate from Regulated Bank Accounts
- Requiring the first deposit or transaction to be made through a bank account registered in the customer's name, held at a financial institution that follows equivalent CDD standards.
8. Ongoing Source of Funds Verification
- For high-risk customers, the company may periodically request updated source of funds documentation, even if transaction patterns remain unchanged.

By applying these EDD measures, LOTOSTORM B.V. (163910) ensures heightened oversight of higher-risk customers, strengthening its AML/CTF/CPF compliance efforts and preventing financial crime activities.

9.6. Timing of CDD Measures

LOTOSTORM B.V. (163910) implements Customer Due Diligence (CDD) measures in a timely manner to ensure compliance with AML/CTF/CPF regulations.

CDD Requirements Based on Transaction Thresholds

- Initial Identification Measures – At the time of account registration, the Company collects and verifies at least the minimum personal details of the player, including:
 - Full name
 - Permanent residential address
 - Date of birth
 - Politically Exposed Person (PEP) screening
 - Sanctions screening
- Threshold for Full CDD Verification – the Company verifies the customer's identity before processing any financial transactions equal to or exceeding NAF 4,000. This threshold applies to:
 - Single transactions reaching NAF 4,000.
 - Multiple linked transactions (deposits, withdrawals, and peer-to-peer transfers) that cumulatively reach NAF 4,000.
 - The threshold is calculated daily, considering all player transactions since the business relationship was established.

- Customer Risk Assessment – Once a player reaches the NAF 4,000 threshold, the Company assesses the customer's risk level and complete any remaining CDD obligations.

Best Practices for Timely CDD Implementation

- Conducting CDD Early – It is recommended to complete full verification at the time of account creation, rather than waiting for the threshold to be met. This reduces the risk of accepting illicit funds before due diligence is complete.

Transaction Restrictions While CDD is Pending

While awaiting necessary documentation or verification, customers may continue using their gaming account under the following conditions:

- If the NAF 4,000 threshold is reached due to a deposit, the player cannot deposit or withdraw additional funds, but may continue playing with existing account funds.
- If the NAF 4,000 threshold is reached due to a withdrawal request, the account must be fully frozen, preventing any further gaming activity.

Failure to Provide CDD Documentation

If the player fails to submit the required CDD documents within 30 days of reaching the NAF 4,000 threshold, the Company does:

- Terminate the business relationship with the player.
- Report the transaction to the FIU if there is a presumption of money laundering or terrorist financing.
- If no suspicion of ML/TF exists, the company returns the funds to the original deposit source (same bank account or digital wallet).
- If ML/TF suspicion exists, the Company's internal procedures determines whether the funds should be blocked, ensuring compliance with AML/CTF regulations.

Consideration of Tipping-Off Risks

- Blocking an account may raise suspicion and tip off the customer. The Company carefully assesses the situation and follow internal procedures to handle the case in compliance with AML regulations.

By implementing these timely CDD measures, LOTOSTORM B.V. (163910) ensures regulatory compliance, reduces financial crime risks, and upholds secure and transparent operations in both online and land-based gaming environments.

9.7. Existing Clients

LOTOSTORM B.V. (163910) applies Customer Due Diligence (CDD) measures not only to new customers but also to existing customers, based on materiality and risk assessment. The company must ensure that its current CDD procedures are sufficient to meet its obligations as outlined in this chapter.

Review of Existing Customer CDD Compliance

- Ongoing Due Diligence – If the Company has already implemented sufficient CDD procedures, it continues applying them while placing special emphasis on ongoing monitoring obligations as detailed in this chapter.
- Risk-Sensitive Approach – For existing customer relationships where prior CDD procedures were inadequate or incomplete, the Company does:
- Apply CDD measures retrospectively, prioritizing higher-risk customers.
- Conduct customer due diligence at appropriate intervals, ensuring compliance with AML/CTF/CPF regulations.

When the CDD is reapplied to Existing Customers

- When there is a significant change in a customer's risk profile (e.g., sudden large transactions, change in jurisdiction, PEP status).
- When regulatory updates or legal obligations require a reassessment of existing customer data.
- If an existing customer engages in transactions that meet or exceed the NAF 4,000 threshold, requiring full CDD verification.

Compliance Obligations for Previously Unverified Customers

- If the Company previously had no formal CDD procedures in place, it must:
- Implement CDD measures for all existing customers, prioritizing those who pose a higher risk.
- Apply CDD at appropriate times using a risk-sensitive approach.

By ensuring that existing customer relationships are compliant with AML/CTF/CPF regulations, LOTOSTORM B.V. (163910) reinforces its commitment to financial security and mitigates money laundering and terrorist financing risks.

9.8. Termination of Relationships

If a player engages in suspicious activities or fails to provide the required customer due diligence (CDD) information, LOTOSTORM B.V. (163910) reserves the right to terminate the business relationship.

Conditions for Termination

A player's account may be terminated if they:

- Are involved in suspicious financial activities.
- Fail to provide adequate CDD documentation within the required timeframe.
- Are identified as posing a high risk of money laundering (ML) or terrorist financing (TF).

Process for Termination

- The decision to terminate a business relationship must be documented and approved by senior management.
- Upon termination, the Company conducts a comprehensive review of the player's activities.
- Any suspicious transactions identified during the review are reported to the Financial Intelligence Unit (FIU).
- All records related to the terminated account are securely stored for a minimum of five years to comply with regulatory requirements.

By enforcing strict termination policies, LOTOSTORM B.V. (163910) ensures compliance with AML/CTF/CPF regulations, preventing potential financial crime risks while maintaining a secure and transparent gaming environment.

9.9. Third-Parties Usage for CDD

LOTOSTORM B.V. (163910) may rely on third parties to perform certain elements of Customer Due Diligence (CDD). However, this reliance is subject to strict regulatory conditions to ensure compliance with AML/CTF/CPF requirements.

Conditions for Relying on a Third Party for CDD

The Company retains ultimate responsibility for ensuring that all CDD measures are effectively implemented, even when relying on a third party. The following conditions must be met:

Immediate Access to CDD Information

- The Company receives all relevant customer identification details (elements a-c) from the third party immediately upon request.

Formal Agreement with the Third Party

- The Company has an agreement that ensures:
- Copies of identification data and relevant documentation are provided upon request.
- This arrangement is periodically tested to confirm compliance.
- Despite relying on a third party, the Company remains responsible for:
- Conducting customer-based risk assessments.
- Determining PEP status.
- Ongoing transaction monitoring.

Third Party Must Be Regulated and Supervised

- The third party must be subject to AML/CFT regulations, monitoring, and compliance measures.
- The third party should have an independent business relationship with the customer, separate from the relationship established with the Company.

Consideration of Country Risk

- Before relying on a third party, the Company makes an assessment of the level of risk associated with the third party's jurisdiction, using available risk intelligence.

Difference Between Third-Party Reliance and Outsourcing

- Third-Party Reliance – The third party performs elements of CDD independently, but the Company remains responsible for compliance.
- Outsourcing Scenario – A third party applies CDD on behalf of the Company, using the Company's policies and procedures. In this case:
- The Company remains fully accountable for ensuring compliance.
- Regular quantitative and qualitative assessments are conducted to evaluate the service provider's effectiveness.
- Customer risk assessments and business relationship decisions are not outsourced—these remain the Company's responsibility.

By enforcing strict oversight over third-party CDD processes, LOTOSTORM B.V. (163910) ensures compliance with AML/CTF regulations, reducing risks while maintaining a secure and legally compliant gaming operation.

10. Suspicious Activity Reporting

LOTOSTORM B.V. (163910) is committed to detecting and reporting any unusual activity that may indicate potential money laundering (ML) or terrorist financing (TF). Such activities typically involve deviations from a customer's normal transaction behavior, frequent high-value transactions, or dealings with high-risk jurisdictions or entities.

To ensure proactive monitoring, all employees receive AML/CTF training and are required to immediately escalate any suspicious behavior or transaction patterns to the designated Compliance Officer.

Role of the Compliance Officer

The Compliance Officer plays a critical role in investigating flagged transactions and behaviors. Their responsibilities include:

- Conducting detailed reviews of unusual activities to determine whether they align with recognized risk indicators.
- Assessing whether a transaction lacks economic or legal justification or poses AML/CTF risks.
- Filing a Suspicious Activity Report (SAR) with the Financial Intelligence Unit (FIU) when required under Curaçao's AML/CTF regulatory framework.

Definition and Examples of Unusual Activity

An unusual transaction is any financial activity that deviates significantly from a customer's known transaction history or does not align with legitimate business practices. These may include:

- Unexpectedly large transactions inconsistent with a customer's usual spending or deposit patterns.
- Frequent high-value transactions or multiple small transactions structured to evade detection thresholds.
- Dealings with unknown entities or transactions involving high-risk jurisdictions with weak AML/CTF controls.
- Unjustified transactions, such as large deposits immediately followed by withdrawals, suggesting attempts to disguise illicit funds.

To enhance detection, the company employs sophisticated transaction monitoring systems that analyze financial behavior in real-time. Any flagged transactions are escalated to the Compliance Officer for further review.

Confidentiality in Reporting

LOTOSTORM B.V. (163910) enforces strict confidentiality regarding Suspicious Activity Reports (SARs) to protect the integrity of investigations. Employees and authorized personnel are strictly prohibited from disclosing SAR-related information to:

- The affected client or their associates.
- Unauthorized personnel inside or outside the company.

Maintaining confidentiality is essential to:

- Prevent tipping-off – Disclosing an investigation could allow suspects to alter their behavior or destroy evidence, undermining enforcement efforts.
- Ensure effective regulatory action – Authorities must be able to conduct thorough investigations without interference.

All SAR-related communications are handled exclusively by the Compliance Officer and authorized personnel, ensuring a secure reporting process.

Consequences of Breaching Confidentiality

Any breach of confidentiality related to SARs is considered a serious violation of the company's AML/CTF policies. Consequences may include:

- Disciplinary actions, including possible termination of employment.
- Legal consequences for both the individual and the company under Curaçao's AML/CTF laws.

By enforcing strict confidentiality measures and adhering to regulatory protocols, LOTOSTORM B.V. (163910) ensures that its AML/CTF compliance efforts remain effective, secure, and legally compliant, reinforcing its commitment to combating financial crime.

11. Compliance Officer

The Compliance Officer plays a critical role in safeguarding the company from money laundering (ML), terrorist financing (TF), and proliferation financing (PF) risks. Their main duties include:

1. AML Program Development and Oversight

- Designing and implementing the company's AML compliance program.
- Ensuring adherence to local and international AML/CTF laws and regulations.
- Conducting periodic reviews of policies and procedures to verify compliance.

2. Staff Training and Awareness

- Organizing training programs to educate employees on AML/CTF compliance requirements.
- Updating staff on new regulations and financial crime risk indicators.

3. Transaction Monitoring and Reporting

- Analyzing transactions to detect suspicious or unusual activities.
- Assessing transactions against reporting indicators established in the Ministerial Decree on Unusual Transactions.
- Reviewing internal reports of unusual transactions for completeness and accuracy.
- Maintaining records of both internally and externally reported unusual transactions.
- Determining when suspicious activity reporting (SAR) warrants blocking/freezing of accounts, while ensuring compliance with anti-tipping-off regulations.
- Conducting deeper investigations into potentially suspicious transactions.
- Preparing and submitting external reports of unusual transactions to the Financial Intelligence Unit (FIU).

4. AML Program Enhancements and Regulatory Compliance

- Making necessary updates to the AML/CTF framework in response to regulatory changes.
- Staying informed on global AML/CTF developments and recommending improvements to management.
- Preparing periodic reports on the company's AML/CTF compliance efforts, including progress updates and risk assessments.

Ensuring Compliance with Curaçao AML Regulations

By fulfilling these key responsibilities, the Compliance Officer plays a pivotal role in:

- Protecting the company from financial crime risks.
- Ensuring strict compliance with Curaçao's AML/CTF regulations.
- Maintaining a robust framework for detecting, preventing, and reporting money laundering and terrorist financing activities.

Through proactive monitoring, staff training, and policy oversight, the Compliance Officer reinforces LOTOSTORM B.V. (163910)'s commitment to legal compliance and financial integrity in the iGaming sector.

12. Employee Training

At LOTOSTORM B.V. (163910), we have developed a comprehensive Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) training program to ensure that all employees are equipped with the necessary knowledge and skills to identify and prevent financial crimes. This training is a crucial component of our compliance framework, ensuring that our staff members understand their legal obligations, recognize suspicious activity, and follow established reporting procedures. An informed workforce is essential to the successful implementation of AML/CTF/CPF policies, reinforcing both the integrity of the company and the credibility of the gaming industry as a whole.

The training program is designed to be role-specific, meaning that employees receive education tailored to the risks they are most likely to encounter. It is mandatory for all employees, regardless of their position within the company. Senior management is trained on high-level policy implementation and strategic oversight, while compliance officers receive in-depth instruction on regulatory requirements and transaction monitoring. Customer-facing staff, operational personnel, and finance teams are also trained to recognize red flags, enforce customer due diligence (CDD) measures, and handle transaction reviews effectively. Since employees at all levels contribute to the company's compliance efforts, their participation in AML/CTF/CPF training is essential.

New employees undergo comprehensive AML training upon joining the company, ensuring that they are fully aware of our compliance policies from the outset. Additionally, all employees must participate in refresher courses at least once per year to stay updated on evolving AML/CTF/CPF regulations and best practices. For employees in roles that involve higher exposure to financial crime risks, such as compliance officers or customer verification personnel, additional training sessions are provided more frequently to reinforce key concepts and address emerging threats.

The training curriculum covers a broad range of topics, ensuring that employees have a well-rounded understanding of financial crime risks and prevention measures. Employees are educated on the specific AML/CTF/CPF laws and regulations applicable to Curaçao, as well as the company's internal policies and procedural requirements. They learn about their responsibilities in maintaining compliance, including conducting proper customer identification and verification through Know Your Customer (KYC) and Customer Due Diligence (CDD) processes. The training also teaches employees how to identify and report suspicious activity, such as unusual transaction patterns, structured deposits and withdrawals, or dealings with high-risk jurisdictions. In addition to these fundamental topics, the program includes guidance on record-keeping requirements, the consequences of non-compliance, and the latest trends in money laundering, terrorist financing, and proliferation financing.

To ensure the training program is engaging and effective, a variety of delivery methods are used. Employees participate in in-person workshops that provide hands-on experience with real-world compliance scenarios, while online courses and e-learning modules allow them to study key concepts at their own pace. Interactive elements such as case studies, role-playing exercises, and transaction simulations help reinforce the learning experience, making it easier for employees to apply their knowledge in day-to-day operations. This combination of instructional methods accommodates different learning styles and enhances retention, ensuring that employees remain well-equipped to fulfill their compliance responsibilities.

Training sessions are conducted by qualified AML professionals, including internal compliance officers and external consultants with expertise in financial crime prevention. These experts ensure that training content remains up to date with the latest legal requirements, regulatory changes, and emerging risks in the industry. By maintaining a structured and evolving AML/CTF/CPF training program, LOTOSTORM B.V. (163910) fosters a culture of compliance, enabling employees to play an active role in detecting and preventing financial crimes while ensuring full adherence to regulatory obligations.

13. Record Keeping

LOTOSTORM B.V. (163910) maintains a comprehensive record-keeping framework to ensure full compliance with Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulations. Our approach prioritizes data security, accessibility, and regulatory adherence, guaranteeing that all relevant records are properly maintained and safeguarded.

To meet record-keeping standards, we retain key documentation for a minimum of five years, in accordance with Curaçao's financial compliance regulations. This includes customer identification records, transaction data, suspicious activity reports (SARs), training records, and internal audit logs. These records serve as a critical reference point for regulatory audits and investigative reviews, ensuring transparency in our operations and facilitating cooperation with financial authorities.

Security is a core component of our data management strategy. All records are encrypted and stored using secure access controls to prevent unauthorized access or tampering. Only authorized personnel have access to sensitive compliance data, and their activities are logged to maintain accountability. Regular security audits are conducted to verify the integrity of stored records and identify any potential vulnerabilities, reinforcing our commitment to data protection and confidentiality.

To streamline record management, we employ a systematic classification and retrieval process, allowing quick and efficient access to relevant documentation when needed. This structure ensures that authorized employees and regulatory bodies can promptly

retrieve information during audits, compliance reviews, or investigations. In addition to secure storage, the company implements continuous internal monitoring and periodic external audits to ensure that our record-keeping practices remain aligned with evolving AML/CTF/CPF regulations.

By maintaining structured and secure records, LOTOSTORM B.V. (163910) not only fulfills its legal obligations but also strengthens internal auditing processes and operational transparency. Our diligent record-keeping practices contribute to the integrity of the gaming industry, reinforcing our commitment to regulatory compliance and ethical business conduct.

14. Independent Audit

To ensure compliance with the new gaming regulations in Curaçao, LOTOSTORM B.V. (163910) undergoes an independent audit that focuses on Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF). This audit provides an in-depth assessment of the company's AML/CTF/CPF framework, helping to identify weaknesses, strengthen risk management strategies, and align with the latest legal requirements. Additionally, the audit process is subject to review by the Curaçao Gaming Control Board, which oversees compliance for all licensed operators.

The primary objective of the annual AML/CTF/CPF audit is to assess the effectiveness of the company's compliance measures and ensure that all legal obligations are met. By conducting regular audits, LOTOSTORM B.V. (163910) is able to stay ahead of emerging financial crime risks, implement best practices, and maintain a robust risk mitigation system. The audit covers several key areas, including risk assessments, transaction monitoring, staff training, and reporting procedures, ensuring that the company is fully compliant with AML/CTF/CPF regulations.

Engagement of an Independent Auditor

To maintain objectivity, the company engages an independent external auditor or, in some cases, an internal audit team with specialized AML/CTF/CPF expertise. This auditor operates separately from the AML Compliance team to eliminate any conflicts of interest. The auditor's qualifications, industry experience, and credibility are carefully evaluated before engagement, ensuring they meet the Curaçao Gaming Control Board's approval standards. The Gaming Control Board must formally approve the selected auditor to ensure compliance with regulatory expectations.

Scope of the AML/CTF/CPF Audit

The audit follows international compliance standards and adheres to the specific AML/CTF/CPF guidelines set by the Curaçao Gaming Control Board. The review

includes an extensive examination of the company's financial crime prevention framework, covering the following areas:

Evaluation of AML/CTF/CPF Policies and Procedures

- The auditor assesses whether the company's AML policies are updated, effective, and aligned with the latest regulatory requirements.
- The review ensures that internal controls mitigate financial crime risks efficiently.

Risk Management Assessment

- The company's risk assessment methodology is examined to determine whether it effectively identifies and addresses high-risk transactions, customers, and jurisdictions.

Transaction Monitoring and Reporting Review

- The auditor evaluates the company's transaction monitoring system to ensure it can detect, flag, and report suspicious activities.
- Effectiveness in filing Suspicious Activity Reports (SARs) to the Financial Intelligence Unit (FIU) is assessed.

Staff Training Evaluation

- The audit examines whether employees receive adequate AML/CTF training, ensuring that all staff members understand their compliance obligations and can recognize suspicious financial activity.

Customer File Review and Due Diligence Compliance

- The auditor conducts a randomized review of customer files to verify adherence to Know Your Customer (KYC), Know Your Business (KYB), and Customer Due Diligence (CDD) standards.
- This review ensures that customer onboarding processes comply with regulatory identity verification and risk assessment requirements.

Reporting Mechanism Audit

- The procedures for filing SARs and other compliance reports are analyzed to ensure they meet the legal standards set by Curaçao's FIU and Gaming Control Board.

Audit Findings and Corrective Actions

Following the audit, the independent auditor prepares a detailed report outlining their findings, recommendations, and any identified compliance issues. This report is submitted to senior management and the Gaming Control Board. If the audit identifies weaknesses or non-compliance areas, the company must implement corrective actions within a specified timeframe. In certain cases, follow-up audits may be required to ensure that necessary improvements have been effectively applied.

Oversight by the Curaçao Gaming Control Board

As the regulatory authority overseeing AML/CTF/CPF compliance, the Curaçao Gaming Control Board conducts its own examinations and reviews audit results to ensure that licensed operators comply with AML regulations. The Board has the authority to request additional documentation, perform inspections, and evaluate the company's implementation of audit recommendations.

The Board's examination process may include:

- Audit Report Review – The Board will analyze the auditor's findings to assess the company's level of compliance and identify any unresolved concerns.
- Interviews and Documentation Analysis – Compliance officers, senior management, and relevant employees may be interviewed to ensure the company is implementing proper AML practices and adhering to legal requirements.

Potential Consequences of Non-Compliance

If LOTOSTORM B.V. (163910) is found non-compliant based on audit results or regulatory reviews, the company may face severe penalties, including:

- Fines imposed by the Gaming Control Board.
- Operational restrictions limiting gaming activities until compliance is restored.
- Suspension or revocation of the gaming license in cases of repeated or serious violations.

To prevent compliance failures, the company works closely with the Gaming Control Board to ensure that all corrective actions are implemented and that regulatory expectations are fully met.

Commitment to AML/CTF/CPF Compliance

By conducting regular independent audits and maintaining strict oversight from the Gaming Control Board, LOTOSTORM B.V. (163910) demonstrates its commitment to financial crime prevention and regulatory transparency. The audit process serves as a proactive measure to enhance the company's AML/CTF/CPF framework, ensuring that risks are effectively mitigated while maintaining the highest standards of integrity within the iGaming industry.

15. Annexes

Annex 1. Abbreviations

AML – Anti-Money Laundering, a framework of regulations and policies designed to prevent financial crimes.

BoD – Board of Directors of the Company, responsible for governance and oversight of compliance measures.

CFATF – The Caribbean Financial Action Task Force, a regional body of 24 Caribbean, Central, and South American states focused on combating money laundering and terrorist financing.

Compliance Officer – A senior management member responsible for detecting and preventing money laundering, terrorist financing, and proliferation financing risks, operating independently from gaming operations.

CTF – Counter-Terrorism Financing, the process of identifying and preventing the funding of terrorist activities.

CPF – Counter-Proliferation Financing, measures aimed at preventing financial support for the spread of weapons of mass destruction.

CDD – Customer Due Diligence, procedures used to verify customer identity and assess financial risk.

EDD – Enhanced Due Diligence, additional verification and risk assessment measures applied to high-risk individuals or entities.

FIU – Financial Intelligence Unit of Curaçao, as defined in Article 2 of the NORUT, responsible for analyzing and processing reports on suspicious financial transactions.

KYB – Know Your Business, a process for verifying and understanding business entities to ensure compliance.

KYC – Know Your Customer, policies and procedures to verify the identity of customers and monitor their financial activities.

SOF/SOW – Source of Funds/Source of Wealth, verification of the origin of financial assets to prevent money laundering.

UBO – Ultimate Beneficial Owner, the individual who ultimately owns or controls an account or transaction.

SAR/STR – Suspicious Activity Report/Suspicious Transaction Report, official reports submitted to regulatory authorities when financial transactions appear suspicious.

PEP – Politically Exposed Person, an individual with a high-profile political or public function, requiring additional scrutiny due to increased risk of financial crimes.

UN – United Nations, an international organization that develops and enforces measures against money laundering and terrorist financing.

EU – European Union, a political and economic union with AML/CTF directives applicable to its member states.

UK – United Kingdom, which enforces its own AML/CTF regulations and financial crime compliance measures.

US – United States, with financial crime regulations overseen by agencies such as OFAC and the Financial Crimes Enforcement Network (FinCEN).

OFAC – Office of Foreign Assets Control, a U.S. Treasury Department agency responsible for enforcing economic sanctions.

FATF – Financial Action Task Force, an international organization that establishes global AML and CTF standards and maintains lists of high-risk jurisdictions.

NOOGH – National Ordinance on Offshore Games of Hazard, Curaçao legislation governing offshore gaming activities.

Annex 2. Definitions

Money Laundering

Money laundering is the process of disguising illicitly obtained funds to make them appear legitimate. It typically involves three stages:

1. Placement – Introducing illicit funds into the financial system.
2. Layering – Conducting complex transactions to obscure the origin of the funds.
3. Integration – Reintroducing laundered money into the legitimate economy.

AML Policy

An AML policy is a formal framework of internal policies, procedures, and controls designed to prevent money laundering and terrorist financing. It is managed by the AML compliance team, led by the Money Laundering Reporting Officer (MLRO), who is responsible for overseeing AML training and conducting independent audits.

Anti-Money Laundering and Counter-Financing of Terrorism Program (AML/CTF/CPF Program)

A structured program developed to prevent financial crime, consisting of internal policies, risk assessments, monitoring systems, and reporting mechanisms. The MLRO oversees the program, ensuring compliance with legal requirements and regulatory best practices.

Money Laundering Reporting Officer (MLRO)

The MLRO is the designated officer responsible for implementing AML policies, monitoring financial transactions, filing Suspicious Transaction Reports (STRs), and ensuring regulatory compliance.

Alerts and Transaction Monitoring

An alert is a notification triggered by predefined red flags, requiring further investigation. Transaction monitoring systems detect potential financial crime by analyzing patterns and identifying anomalies.

Regulatory Bodies and Supervisory Authorities

- Curaçao Gaming Control Board (GCB): The primary AML/CTF supervisory authority for the gaming sector.
- Financial Intelligence Unit (FIU): The national agency responsible for receiving, analyzing, and escalating reports on suspicious transactions.
- Financial Action Task Force (FATF): An international body that establishes AML/CTF guidelines and maintains blacklists and greylists for non-compliant countries.

Know Your Customer (KYC) and Due Diligence Measures

- KYC: Policies and procedures for verifying a customer's identity and assessing their transaction patterns.
- Customer Due Diligence (CDD): A process that involves verifying identities, assessing risk, and monitoring transactions for suspicious activity.
- Enhanced Due Diligence (EDD): Additional verification steps for high-risk customers, including obtaining information on source of wealth and business activities.

Sanctions Compliance and Screening

- Beneficial Owner: The person who ultimately controls an account or transaction.
- Sanctions: Restrictions imposed on countries, individuals, or entities due to security concerns, including trade bans and asset freezes.
- Automated Screening Tools (AST): Software used to screen customers against sanctions lists and flag restricted entities.
- Blacklist: A list of entities, individuals, or locations subject to financial restrictions.
- Comprehensive Sanctions: Measures prohibiting all financial dealings with a sanctioned country, except in rare exceptions.

Risk Management and Financial Crime Prevention

- Risk-Based Approach (RBA): A methodology for assessing and managing financial crime risks based on transaction types, customers, and jurisdictions.

- Risk Appetite: The level of risk an institution is willing to accept within its operations.
- High-Risk Third Country: A country designated by FATF or the European Commission as posing an elevated AML/CFT risk.
- Economic Sanctions: Trade or financial restrictions imposed by governments to influence political or economic behavior.

Record-Keeping and Reporting Obligations

- Suspicious Transaction Report (STR): A formal report submitted to the FIU when a transaction raises AML/CTF concerns.
- Unusual Transaction: Any transaction that deviates from expected patterns, potentially indicating illicit activity.
- Audit Logs: Records maintained for at least five years, documenting AML compliance efforts.
- First Line of Defense: Employees responsible for collecting customer information and identifying suspicious activity during onboarding.

Money Laundering Techniques and Prevention Measures

- Structuring: The process of making multiple smaller transactions to evade reporting thresholds.
- Layering: The act of moving illicit funds through multiple transactions to obscure their origin.
- Integration: The final stage of money laundering, where funds appear fully legitimate.
- Sanctions Evasion: Attempts to conceal transactions involving sanctioned entities to bypass financial restrictions.

International Cooperation and AML Standards

- Office of Foreign Assets Control (OFAC): A U.S. agency enforcing economic sanctions.
- Egmont Group of FIUs: A global network of Financial Intelligence Units that facilitates AML/CTF information exchange.
- The Wolfsberg Group: An association of global banks that develops best practices for private banking AML compliance.