

DOUBLED B.V.

AML/CTF/CPF POLICY

Registration Number 166107

17, Chuchubiweg, Willemstad, Curacao

24/03/2025

APPROVED BY THE BOARD OF DIRECTORS

A handwritten signature in blue ink, consisting of a large, stylized 'A' followed by a horizontal line and a small flourish.

Next Review: 24/03/2026

Compliance Officer:

Sergey Volf

compliance@doubledbv.com

Table of Contents

- 1. Statement**
- 2. iGaming Environment**
- 3. Money Laundering**
- 4. Terrorist Financing**
- 5. Proliferation Financing**
- 6. Money Laundering, Terrorist Financing, Proliferation Financing
Risks Management**
 - 6.1. Curaçao Legislation & Compliance**
 - 6.2. Risk-Based Approach**
 - 6.3. Risks in Technological Development**
- 7. Client Due Diligence**
- 8. Suspicious Activity Reporting**
- 9. Sanctions**
- 10. Compliance Officer**
- 11. Senior Management**
- 12. Training & Record Keeping**
- 13. AML/CTF/CPF Audit**
- 14. Abbreviations & Definitions**

1. Statement

DOUBLED B.V. has implemented an Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing Policy (AML/CTF/CPF Policy) to address and mitigate risks associated with money laundering and terrorism financing. This policy aligns with both domestic and international standards for AML/CTF/CPF compliance and ensures adherence to relevant regulations. It provides a robust framework to manage risks related to customer interactions, product and service offerings, payment channels, geographic regions, and operational delivery methods.

The Board of Directors (BoD) at DOUBLED B.V. holds responsibility for approving, implementing, and overseeing the AML/CTF/CPF Policy. This policy undergoes annual reviews to ensure it remains current and is updated as necessary to reflect significant changes in regulations or operational procedures. Additionally, urgent amendments may be proposed by an appointed officer in response to recommendations from internal or external AML audits, considering the associated risks and impacts.

DOUBLED B.V.'s AML/CTF/CPF Policy is structured to comply with the core international and Curaçao-specific regulations, including the National Ordinance for Games of Chance (LOK), the Criminal Code of Curaçao, the National Ordinance on Offshore Games of Hazard (NOOGH), the National Ordinance Penalization of Money Laundering (NOPML), the National Ordinance on the Reporting of Unusual Transactions (NORUT), and the National Ordinance on Identification when Rendering Services (NOIS), as amended up to May 16, 2024. It also incorporates the requirements of the Sanctions National Ordinance (SNO) and the Kingdom Sanction Act.

Further, this policy reflects international best practices and guidelines, including the Financial Action Task Force (FATF) Recommendations, the European Union's Anti-Money Laundering Directives (4th, 5th, and 6th AMLDs), and the Wolfsberg Principles.

In summary, the AML/CTF/CPF Policy of DOUBLED B.V. is designed to meet the standards set by the Curaçao Gaming Control Board, the country's AML/CTF/CPF supervisory authority. All directors, officers, employees, and third-party consultants involved in auditing are required to adhere to and uphold the principles detailed within this policy.

2. iGaming Environment

DOUBLED B.V. (166107), a legally registered entity based in Curaçao, is the owner and operator of the website <https://portebet.com>. The company operates under an official online gaming license issued by the Curaçao Gaming Control Board, specifically license number OGL/2024/1015/0870. This license is granted in compliance with stringent regulatory requirements and standards set forth by the Curaçao regulatory authorities. As part of its commitment to regulatory compliance, DOUBLED B.V. adheres to all licensing obligations, including the imposition of geographical restrictions to ensure lawful operations within permitted markets.

The Curaçao Gaming Control Board mandates that all licensed remote gaming operators, including DOUBLED B.V., are prohibited from offering their services in jurisdictions where online gambling is either explicitly illegal or where local regulations restrict such activities. These restricted jurisdictions include, but are not limited to, the United States, Australia, Dutch West Indies (Aruba, Bonaire), Curaçao, France, Germany, the United Kingdom, Belize, and the Netherlands. DOUBLED B.V. strictly complies with these regulations by refraining from targeting or providing services to customers in these regions. This ensures that the company's activities remain within the confines of both domestic and international legal frameworks.

To reinforce its compliance measures, DOUBLED B.V. actively monitors changes in local and international gambling regulations. This ensures that the company operates only in jurisdictions where online gaming and gambling activities are explicitly permitted and avoids marketing or offering its services to customers in countries where such activities are banned or otherwise restricted. The company also employs advanced technological solutions to block access from prohibited regions, safeguarding against unintentional violations of regulatory boundaries.

As an e-gaming and betting operator, DOUBLED B.V. acknowledges and proactively addresses the inherent risks associated with money laundering and financial crimes within the online gaming industry. These risks include, but are not limited to, identity theft, fraudulent activities, structuring (the practice of breaking down large transactions into smaller, less detectable amounts), layering (the use of complex transaction patterns to disguise the origins of funds), and the potential for collusion between internal employees and external parties, such as customers or third-party payment providers, to exploit vulnerabilities in security protocols.

DOUBLED B.V. has implemented a robust framework of anti-money laundering (AML) and counter-terrorism financing (CTF) measures, as detailed in its company policies. These measures include comprehensive customer due diligence (CDD) procedures, regular staff training on AML/CTF practices, and continuous monitoring of transactions to detect and prevent suspicious activities. The company also

enforces strict know-your-customer (KYC) protocols to verify customer identities and ensure compliance with applicable legal standards. Additionally, partnerships with trusted payment providers and the use of secure transaction methods further minimize the risk of financial crimes.

DOUBLED B.V. is dedicated to maintaining the highest standards of integrity and accountability in its operations. By aligning its practices with local and international regulatory requirements, the company seeks to build trust with its customers, regulatory authorities, and other stakeholders. These efforts underscore DOUBLED B.V.'s commitment to operating a secure, transparent, and legally compliant online gaming platform.

3. Money Laundering

Money laundering constitutes a cornerstone of financially motivated crime and often operates on a global scale, spanning international jurisdictions. It facilitates a broad range of illegal activities, including tax evasion, breaches of international sanctions, fraud, corruption, illegal arms trading, drug trafficking, extortion, and kidnapping. The primary aim of money laundering is to conceal the illicit origins of funds derived from these crimes, disguising their identity, source, and final destination to integrate them seamlessly into the legitimate economy.

Key Stages of Money Laundering

- 1. Placement**

Placement is the initial phase in the money laundering process, where unlawfully obtained funds are introduced into the financial system. Common methods include depositing cash into financial institutions, purchasing high-value goods, or engaging in financial transactions designed to initiate the integration of illegal funds into legitimate channels. The objective of this phase is to make the funds appear to originate from a lawful source.

- 2. Layering**

During the layering phase, the illicit funds undergo a series of complex transactions aimed at obscuring their origins. This may involve multiple transfers between bank accounts, converting money into various currencies, investing in diverse financial products, or leveraging offshore accounts. These actions create an intricate web of financial activity, making it challenging for investigators to trace the funds back to their criminal source.

- 3. Integration**

The final stage of money laundering is integration, where the laundered funds are reintroduced into the legitimate economy. This is accomplished through

activities such as purchasing luxury goods, investing in high-value assets, or acquiring businesses that deal with substantial cash flows. At this stage, the money appears legitimate, making its illicit origins extremely difficult to detect.

Risks in Online Gambling Platforms:

Money laundering activities can occur at any stage, and online gambling platforms are particularly vulnerable to exploitation during these processes. This 41 underscores the critical importance of preventing anonymous transactions and ensuring the company does not facilitate suspicious financial activities.

Relation to Terrorist Financing:

Terrorist financing refers to the financial support of terrorist activities. Unlike money laundering, the origin of these funds may be entirely legitimate; however, the methods used to channel these funds often mimic laundering techniques. For example, prepaid cards are frequently used to purchase materials for carrying out attacks. Recognizing this overlap, DOUBLED B.V. ensures its staff remains well-trained and updated on the latest trends and methods used in terrorist financing to safeguard against such risks.

Risk Management and Compliance:

To effectively combat money laundering and related threats, DOUBLED B.V. employs a robust risk management framework. Key strategies include:

- **Verification of Fraud and Identity Theft**
Thorough customer due diligence (CDD) is performed to verify the identity, age, and location of users. This ensures compliance with know-your-customer (KYC) requirements and prevents fraudulent access.
- **Monitoring of Multiple Accounts and High Transaction Volumes**
Systems are in place to detect unusual activity, such as the operation of multiple accounts under the same user or unusually high transaction volumes, which may indicate suspicious behavior.
- **Detection of Illicit Fund Deposits**
The company actively monitors deposits to identify funds that may originate from illegal activities or instances where the platform is used as a temporary holding account for illicit money.
- **Scrutiny of Player-to-Player Transfers**
Player-to-player transfer features are closely monitored to detect misuse for transferring illicit funds or facilitating unauthorized cash-outs.

Continuous Risk Assessment:

This list is not exhaustive, as new risks may emerge over time. DOUBLED B.V. conducts regular risk assessments to identify vulnerabilities specific to its operations and tailors its compliance programs accordingly. The company also prioritizes ongoing training for its employees to ensure the effectiveness of its internal anti-money laundering (AML) and counter-terrorism financing (CTF) measures.

By implementing these comprehensive strategies, DOUBLED B.V. reinforces its commitment to maintaining a secure and transparent operational environment, ensuring full compliance with local and international regulatory frameworks.

4. Terrorist Financing

Terrorist financing refers to the provision of financial support to individuals, groups, or activities associated with terrorism. These funds may originate from both legal and illegal sources and are critical for carrying out a wide range of operations, from small-scale acts to large-scale attacks. Understanding the mechanisms and indicators of terrorist financing is essential to mitigating the associated risks and ensuring compliance with international regulations.

Sources of Terrorist Financing:

The origins of terrorist financing can be broadly categorized into two primary avenues:

1. Legal Sources

Terrorists may exploit legitimate channels to fund their activities. Common legal sources include:

- Legitimate Businesses: Profits from lawful enterprises can be redirected toward terrorist activities.
- Donations: Charitable contributions, particularly to organizations with inadequate oversight, can be manipulated to funnel money.
- Financial Activities: Lawful transactions, including investments, may be used as fronts for terrorism financing.

2. Illegal Sources

A significant portion of terrorist financing originates from illicit activities, including:

- Drug Trafficking: Profits from the illegal drug trade are frequently redirected to fund terrorism.
- Fraud and Smuggling: Financial fraud, tax evasion, and smuggling provide a steady revenue stream.

- Extortion and Kidnapping: Ransoms and forced payments are direct methods of raising funds.
- Money Laundering: Sophisticated laundering practices are employed to disguise the origins of illicit funds.

Methods of Transferring Funds:

Terrorists utilize a variety of channels to transfer funds, often blending formal and informal systems:

- Formal Channels
Traditional banking and financial institutions are frequently exploited using advanced techniques such as layering (multiple transactions to obscure origins) and structuring (splitting large sums into smaller amounts to avoid detection).
- Informal Channels
Systems operating outside official frameworks, such as hawala networks, are widely used. These informal transfer mechanisms are difficult to track due to their lack of documentation and reliance on trust-based exchanges.

Indicators of Terrorist Financing:

DOUBLED B.V. recognizes the importance of identifying potential indicators of terrorist financing, which may include:

- Unusual transaction patterns that deviate significantly from normal business or personal behavior.
- Frequent or large financial transfers to or from regions considered high-risk for terrorist activity.
- Transactions involving entities or individuals associated with known terrorist organizations.
- High-risk sector involvement, such as cash-intensive businesses, where financial movements lack transparency.
- Financial actions that appear intentionally designed to conceal or obscure their true purpose.

Mitigation Measures and Regulatory Compliance:

To counter the risks associated with terrorist financing, DOUBLED B.V. has implemented robust Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) policies, which include:

- Customer Due Diligence (CDD): Conducting thorough checks on customer identities, verifying documentation, and assessing risk factors.

- Transaction Monitoring: Employing systems to detect unusual patterns or suspicious activities across customer accounts.
- Reporting of Suspicious Activities: Ensuring all detected anomalies are promptly reported to relevant authorities.

DOUBLED B.V. strictly adheres to international sanctions and uses multiple regulatory lists to prevent inadvertently supporting terrorism. These include, but are not limited to:

- Sanctions National Ordinance (SNO)
- Kingdom Sanction Act
- Curaçao Gaming Control Board (GCB) announcements
- Office of Foreign Assets Control (OFAC) and its Specially Designated Nationals (SDN) list
- United Nations Security Council sanctions lists
- European Union (EU) sanctions
- U.S. List of Foreign Terrorist Organizations (FTO)

By cross-referencing these lists, DOUBLED B.V. ensures that its operations remain compliant and do not inadvertently facilitate terrorism.

International Guidelines and Standards

DOUBLED B.V.'s AML/CTF framework aligns with global standards established by key international organizations:

- Financial Action Task Force (FATF): Provides comprehensive recommendations to identify and report suspicious transactions related to money laundering and terrorist financing.
- OFAC (Office of Foreign Assets Control): Enforces U.S. trade and economic sanctions and maintains the SDN list to restrict dealings with individuals and entities involved in terrorism.
- European Union (EU): Mandates member states to implement strict AML/CTF measures and comply with international sanctions to prevent misuse of the financial system.
- United Nations (UN): Imposes global sanctions and maintains a database of individuals and organizations linked to terrorism to curb their access to financial resources.

Commitment to Compliance:

DOUBLED B.V. remains steadfast in its commitment to combating terrorist financing through the application of rigorous policies, employee training, and continuous enhancement of its compliance measures. By adhering to international and local

regulations, the company contributes to global efforts to prevent financial systems from being exploited to support terrorism.

5. Proliferation Financing

Proliferation financing refers to the provision of financial resources or support for the development, acquisition, and distribution of weapons of mass destruction (WMDs), including their delivery systems. This type of financing is a significant threat to global security and is strictly prohibited under international and Curaçao regulations. As an operator in the iGaming sector, DOUBLED B.V. is committed to addressing the risks associated with proliferation financing as part of its broader Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) framework.

Compliance with Curaçao iGaming Regulations:

The Curaçao Gaming Control Board (GCB) has implemented enhanced compliance requirements to address proliferation financing risks, reflecting the evolving global standards. These requirements obligate all licensed operators, including DOUBLED B.V., to identify, mitigate, and report potential risks associated with proliferation financing. Key elements include:

1. Risk Assessment

DOUBLED B.V. conducts regular risk assessments to identify vulnerabilities specific to proliferation financing within its operations. These assessments consider factors such as:

- The use of the platform by customers from high-risk jurisdictions with weak proliferation controls.
- Transactions involving goods, services, or entities linked to WMD proliferation networks.
- Patterns of financial activity consistent with known methods of proliferation financing.

2. Enhanced Customer Due Diligence (CDD)

DOUBLED B.V. implements enhanced CDD measures to verify the identity of customers, particularly those from high-risk jurisdictions. This includes:

- Screening customers against international sanctions lists, including those maintained by the United Nations Security Council, the Financial Action Task Force (FATF), and the European Union.
- Investigating the purpose and intended nature of transactions that deviate from standard patterns.

- Monitoring for customers with affiliations to entities flagged for involvement in proliferation-related activities.
- 3. Transaction Monitoring and Reporting

Advanced transaction monitoring systems are employed to detect unusual or suspicious activity that may indicate proliferation financing. These systems analyze transaction patterns, flag high-risk transactions, and ensure that suspicious activity reports (SARs) are promptly filed with relevant authorities, including the Curaçao Financial Intelligence Unit (FIU).
- 4. Sanctions Screening and Compliance

DOUBLED B.V. strictly adheres to the sanctions and compliance requirements established by Curaçao and international regulatory bodies. This includes:

 - Prohibiting transactions involving individuals, entities, or jurisdictions subject to WMD-related sanctions.
 - Screening all financial transactions and business relationships against updated sanctions lists, including the Kingdom Sanction Act and United Nations Security Council Resolutions.
 - Maintaining detailed records of sanctions screening and reporting results for audit and regulatory review.
- 5. Training and Awareness

Employees at DOUBLED B.V. receive specialized training on proliferation financing risks, including how to identify red flags and respond appropriately. This training ensures that staff remain vigilant and equipped to comply with Curaçao's evolving regulatory landscape.
- 6. Collaboration with Authorities

DOUBLED B.V. works closely with the Curaçao Gaming Control Board, Financial Intelligence Unit (FIU), and other relevant authorities to strengthen compliance. The company ensures full cooperation in investigations, provides timely reporting, and participates in initiatives aimed at combating proliferation financing in the iGaming sector.

Commitment to Global Security:

DOUBLED B.V. recognizes the critical importance of preventing its platform from being misused to facilitate proliferation financing. By adhering to Curaçao's new iGaming compliance requirements and international standards, the company reinforces its commitment to maintaining a secure, transparent, and compliant gaming environment. These efforts contribute to global initiatives aimed at safeguarding financial systems from exploitation by those seeking to develop or distribute weapons of mass destruction.

6. Money Laundering, Terrorist Financing, Proliferation Financing Risks Management

DOUBLED B.V. employs a risk-based approach (RBA) as a cornerstone of its Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) policies. This approach enables the company to allocate resources efficiently and focus on mitigating the most significant risks. In compliance with Curaçao's Law on Offshore Games (LOK)—which replaces the National Ordinance on Offshore Games of Hazard (NOOGH)—DOUBLED B.V. has adopted a robust and comprehensive RBA to ensure compliance with stricter regulatory requirements while maintaining the integrity of the iGaming sector.

6.1 Curaçao Legislation & Compliance

Under the LOK framework, DOUBLED B.V. demonstrates compliance by integrating its RBA into a comprehensive AML/CTF/CPF program tailored to the company's size, nature, and complexity. Key elements include:

- **Employee Training:** Regular training ensures all employees understand their obligations under AML/CTF/CPF regulations, with a specific focus on applying the RBA and managing sector-specific risks.
- **Independent Audits:** External audits assess the effectiveness of the company's AML/CTF/CPF program and the implementation of its RBA. Recommendations are promptly acted upon to improve compliance.

6.2 Risk-Based Approach

At DOUBLED B.V., assessing the potential exposure to money laundering (ML) and terrorist financing (TF) through customer interactions is a fundamental part of our risk-based compliance strategy. This involves carefully reviewing each client's profile, financial activities, and declared sources of wealth to uncover any vulnerabilities that may require enhanced oversight.

Certain customer characteristics are linked with elevated risk. For instance, individuals reporting multiple sources of income may complicate the verification of legitimate fund origins. Likewise, erratic or unpredictable spending behavior can present challenges in risk profiling. Politically Exposed Persons (PEPs) are subject to additional scrutiny due to their potential access to public funds and the inherent corruption risks tied to their positions.

Further high-risk indicators include clients whose spending habits are significantly inconsistent with their reported earnings or those operating multiple gaming accounts—a tactic often used to bypass transaction monitoring or mask financial

activity. To manage these risks effectively, DOUBLED B.V. applies transaction thresholds and behavioral benchmarks aligned with typical customer usage patterns.

In contrast, clients with a single, documented income source and consistent transaction activity are considered lower risk. Customers showing irregular financial behavior or complex income structures are monitored more closely and may be subjected to Enhanced Due Diligence (EDD).

Risks Related to Products, Services, and Transactions:

Certain services, financial tools, and transaction types used within the iGaming sector inherently carry a higher potential for misuse in financial crimes. Criminal actors often exploit areas where compliance controls are weaker, particularly in environments that process large volumes of financial flows.

Illicit funds originating from activities such as fraud, trafficking, or organized theft are sometimes laundered through gaming platforms to disguise their illegal origin. Tools that offer a degree of anonymity—such as prepaid cards, cryptocurrencies, or tokenized digital assets—present a heightened risk due to the challenges in tracing their movement.

Additional concerns arise when player accounts are misused as temporary holding spaces for financial transfers or when peer-to-peer functionalities are exploited to facilitate unauthorized fund movement. Third-party financial instruments, such as payment cards or bank accounts in someone else's name, also pose risks by complicating identity verification. Moreover, services linked to gambling—like currency conversion, credit issuance, or operations spanning multiple platforms—introduce additional compliance risks.

To manage these exposures, DOUBLED B.V. implements robust monitoring protocols, applies EDD measures where needed, and aligns all controls with international AML/CTF/CPF regulatory standards.

Geographic Risk Exposure:

The geographical location of a customer and the source of their funds are important risk indicators. Countries with limited anti-money laundering oversight, known corruption issues, or active international sanctions represent elevated exposure to financial crime and terrorist financing risks. Special consideration is given to regions associated with the proliferation of weapons or support for terrorism.

To assess and manage geographical risk effectively, DOUBLED B.V. refers to credible global sources, including:

- FATF (Financial Action Task Force) lists of high-risk or monitored jurisdictions

- CFATF (Caribbean Financial Action Task Force) advisories on regional threats
- U.S. Department of State's INCSR reports on financial crime trends
- European Commission's list of third countries with strategic AML/CFT deficiencies
- OFAC (Office of Foreign Assets Control) sanctions targeting specific regions or actors
- Transparency International's Corruption Perceptions Index (CPI) for corruption benchmarks

DOUBLED B.V. utilizes a structured framework to classify jurisdictions by risk level. Enhanced Due Diligence is applied to clients from high-risk areas, and activities involving sanctioned territories are restricted or prohibited. This classification system is continuously updated to reflect the latest global data, ensuring compliance and operational transparency.

Channel Risk and Mitigation Measures:

The manner in which customers access DOUBLED B.V.'s services also impacts the level of exposure to financial crime. Channels that offer anonymity or limited identity verification—such as digital interfaces without strong onboarding procedures—pose significant risk if not adequately managed.

To counter this, DOUBLED B.V. enforces strict verification protocols for all interactions, especially those involving anonymous features. Technologies such as biometric verification, advanced identity authentication tools, and secure onboarding mechanisms are used to prevent fraud and confirm the legitimacy of financial activity.

By maintaining high standards of monitoring and applying secure user authentication across all engagement channels, DOUBLED B.V. reinforces its commitment to international compliance and ensures the integrity of its gaming operations against threats of money laundering and terrorist financing.

6.3. Risks in Technological Development

DOUBLED B.V. is firmly committed to ensuring that advances in technology do not become avenues for financial misconduct such as money laundering (ML) or terrorist financing (TF). As technological innovation continues to reshape the iGaming landscape, the company implements a robust risk management framework, backed by rigorous internal controls, to proactively detect and mitigate any vulnerabilities that may emerge from these changes. By incorporating detailed risk evaluations into

every innovation phase—whether related to services, products, or operations—DOUBLED B.V. ensures that its regulatory obligations are upheld without compromise.

Risk Assessment Procedures for Emerging Technologies

To effectively manage the compliance implications of adopting new technologies, DOUBLED B.V. undertakes comprehensive assessments in scenarios including:

- The launch of new gaming features or products
- Operational changes designed to optimize internal processes or improve customer interaction
- Deployment of novel service channels, such as updated payment interfaces or digital access methods
- Integration of cutting-edge technologies, including blockchain systems, AI-based solutions, or advanced security frameworks

Before introducing any such technologies, a thorough review is carried out to evaluate potential risks and exploitability by bad actors. This review process includes identifying possible points of exposure, documenting findings, and mapping outcomes against national and international AML/CTF standards. These evaluations form a critical component of DOUBLED B.V.'s strategy to stay ahead of financial crime risks stemming from technological evolution.

Implementing Controls and Mitigation Strategies

Following the identification of risk areas, DOUBLED B.V. swiftly applies appropriate countermeasures to strengthen its defenses. These may include:

- **Enhanced Security Infrastructure**
Implementation of multi-factor authentication (MFA), biometric verification protocols, AI-driven fraud detection systems, and full-spectrum data encryption to safeguard against unauthorized access or misuse of digital systems.
- **Upgraded Transaction Monitoring**
Investment in intelligent monitoring platforms capable of recognizing atypical transaction patterns and automatically flagging suspicious financial behavior, particularly those that may indicate ML or TF activity.

- **Dynamic Policy Revisions**

Continuous adaptation of internal AML/CTF policies to reflect the new risk vectors introduced by evolving technology. This ensures that DOUBLED B.V.'s compliance protocols remain flexible, responsive, and aligned with the current threat landscape.

Through continuous oversight and adaptation to technological advancements, DOUBLED B.V. reinforces its commitment to maintaining a secure, transparent, and compliant environment. This forward-leaning strategy ensures that innovation does not come at the expense of regulatory obligations or the security of the company's financial operations, allowing DOUBLED B.V. to remain both innovative and compliant in a fast-evolving digital ecosystem.

7. Client Due Diligence

DOUBLED B.V. implements a stringent Customer Due Diligence (CDD) program to prevent the creation of anonymous or fictitious accounts. Verifying the identity of all players and understanding their business relationships are critical components in combating money laundering, terrorism financing, and proliferation financing. These measures also ensure the company's compliance with Curaçao's regulatory requirements. Any suspicious activities identified through CDD are reported promptly to the Financial Intelligence Unit (FIU) and, if necessary, to the Public Prosecutor's Office.

When CDD Measures Are Applied:

CDD measures are applied during specific circumstances to identify and mitigate risks. The company ensures compliance by implementing due diligence protocols when particular thresholds are reached or suspicious activities are detected. For example:

- When transactions amount to NAF 4,000 or more, whether as a single or cumulative amount.
- During occasional transactions exceeding NAF 4,000.
- When there is suspicion of money laundering, terrorism financing, or other illicit activities.
- If discrepancies or uncertainties arise in previously obtained customer information.
- For linked transactions that collectively exceed NAF 4,000, even if individual transactions fall below the threshold.

In situations deemed high-risk, enhanced due diligence (EDD) measures are applied to ensure further scrutiny.

Details of CDD Measures:

The company's CDD process includes identifying and verifying player identities, understanding business relationships, and monitoring transactions. Verification is conducted using legitimate, reliable, and independent documentation or systems. For legal entities, this involves identifying the ultimate beneficial owner (UBO) and examining their ownership and control structure.

Examples of CDD measures include:

- Verifying identities using government-issued photo IDs, utility bills, or bank statements.
- Understanding the nature and purpose of the business relationship with the platform.
- Conducting ongoing monitoring to ensure transactions align with the player's profile and assessing the source of funds when necessary.

The company ensures confidentiality when filing reports to the FIU, avoiding any "tipping-off" of players. If suspicions arise and CDD might alert a player, the process is bypassed, and a report is filed directly with the FIU.

Player Identification and Verification Process:

DOUBLED B.V. collects essential personal details to establish a player's identity and determine their risk level. For low-risk scenarios, basic details are sufficient, but higher-risk situations require more comprehensive information.

The identification process includes gathering the following details:

- Full name.
- Permanent residential address.
- Date and place of birth.
- Nationality.
- Identification number.

Verification is achieved through:

- Government-issued photo IDs, such as passports or national identity cards.
- Supplementary documents, such as utility bills or bank statements no older than six months.
- Communication-based verification, using letters, emails, or phone calls.
- Advanced tools, such as biometric checks, database cross-referencing, IP tracking, and funding method analysis.

If required, additional steps are taken, such as requesting a selfie with the ID or confirming the first deposit through a regulated financial institution.

Understanding the Business Relationship:

Understanding the purpose and nature of the business relationship is an integral part of CDD. For higher-risk customers, DOUBLED B.V. collects detailed documentation regarding the source of wealth, transaction patterns, and expected activity levels to ensure the legitimacy of their activities.

For example:

- High-risk clients: Require comprehensive documentation, including independent verification of sources of wealth.
- Low- and medium-risk clients: May only need a basic employment or business declaration.

This ensures any unusual or suspicious activities are detected early.

Existing Customers CDD & Monitoring:

DOUBLED B.V. applies Customer Due Diligence (CDD) procedures not only at the time of onboarding new clients, but also as an ongoing process throughout the entirety of the customer relationship. This dynamic approach—grounded in continuous monitoring and periodic risk reassessments—ensures that the company remains in full alignment with Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulations. The ongoing nature of this framework reflects DOUBLED B.V.'s broader risk-based strategy to anticipate and address evolving financial crime threats.

Consistent Monitoring and Review:

Ongoing CDD Application

DOUBLED B.V. maintains active due diligence protocols across its entire customer base. Central to this is the continuous review of transaction behavior and the timely reassessment of individual customer risk ratings.

Risk-Responsive Actions:

In cases where initial CDD may have been limited or outdated, the company initiates retrospective reviews. These include:

- Re-verifying and updating information for customers deemed to present elevated risk;
- Scheduling routine data refreshes to ensure compliance with current AML/CTF/CPF standards.

Scenarios That Require Reapplication of CDD:

DOUBLED B.V. reactivates and applies full CDD procedures under specific circumstances, including:

- When a client's risk profile changes significantly—such as conducting unusually large transactions, relocating to a high-risk jurisdiction, or being designated a Politically Exposed Person (PEP);
- When legal or regulatory developments mandate the collection of updated customer information;
- When a previously onboarded customer initiates transactions that meet or exceed the company's defined financial threshold of NAF 4,000, triggering the obligation for full identity verification.

Rectifying Historical CDD Gaps:

For clients who were previously onboarded under less stringent verification requirements, DOUBLED B.V. undertakes the following measures:

- High-risk customers are prioritized for immediate verification;
- Comprehensive CDD reviews are scheduled in line with the customer's risk tier, ensuring that due diligence procedures remain proportionate and effective.

Simplified Due Diligence (SDD):

In low-risk scenarios, Simplified Due Diligence (SDD) measures apply. These measures involve collecting basic customer details and conducting reviews less frequently. While SDD allows for a streamlined process, enhanced measures are implemented immediately if suspicious activities arise or if the player's risk profile changes.

Enhanced Due Diligence (EDD):

EDD measures are applied to high-risk scenarios and situations requiring additional scrutiny. This includes a thorough investigation of a player's background, verification of the source of funds and wealth, and close monitoring of transaction patterns.

EDD is mandatory for politically exposed persons (PEPs) and involves:

- Obtaining senior management approval.
- Conducting in-depth risk assessments.
- Maintaining ongoing monitoring to address elevated risks.

Handling Politically Exposed Persons (PEPs):

DOUBLED B.V. applies heightened scrutiny to PEPs, their families, and close associates to address the increased risks they present. Enhanced Due Diligence measures include:

- Senior management approval prior to account creation or transactions.
- Comprehensive documentation of the source of funds and wealth.
- Rigorous, ongoing monitoring of all activities and transactions.

Timing of CDD Measures:

The company enforces Customer Due Diligence (CDD) measures promptly and in strict adherence to applicable regulations under Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) frameworks. The company ensures that customer identity verification is carried out effectively at key stages of engagement, helping to safeguard the integrity of its financial ecosystem.

Transaction Thresholds Triggering CDD

From the outset of account creation, DOUBLED B.V. collects and verifies essential identifying information from each player. This includes:

- Full legal name
- Residential address
- Date of birth
- Screening against Politically Exposed Person (PEP) lists
- Screening against sanctions lists

As part of its risk-based compliance model, the company mandates identity verification prior to processing any transaction that meets or exceeds NAF 4,000. This requirement is activated in two scenarios:

- A single transaction reaching or surpassing NAF 4,000;
- A series of connected transactions (such as deposits, withdrawals, or internal transfers) that cumulatively amount to NAF 4,000.

To remain vigilant, DOUBLED B.V. aggregates transaction activity per user on a daily basis, monitoring all movements from the start of the customer relationship. When the financial threshold is reached, a full risk assessment is triggered, and any incomplete CDD steps are completed immediately.

Prioritizing Early Due Diligence

DOUBLED B.V. takes a proactive stance by verifying customer identity during the registration phase—regardless of transaction size. This early verification helps prevent unauthorized or suspicious activity before any financial operations occur and reinforces the company's preventative controls.

Interim Restrictions Pending CDD Completion

In instances where the NAF 4,000 threshold is met before full CDD is finalized, the following temporary restrictions are applied:

- If triggered by a deposit: The player is barred from making further deposits or withdrawals but can use their existing balance for gaming purposes.
- If triggered by a withdrawal: The account is temporarily frozen, and all gaming activity is suspended until the verification process is completed.

These measures ensure uninterrupted compliance while maintaining a degree of operational flexibility for non-suspicious customers.

Handling CDD Non-Compliance

If a customer fails to submit the required verification documents within 30 days of hitting the NAF 4,000 threshold, DOUBLED B.V. proceeds with the following actions:

- The player's account is closed, and the business relationship is terminated;
- If there are signs of money laundering or terrorist financing, a Suspicious Transaction Report (STR) is filed with the Financial Intelligence Unit (FIU);
- If no suspicion is present, any remaining balance is refunded to the original source of payment (e.g., bank account or digital wallet);
- If suspicion persists, internal procedures are followed to determine whether funds should be frozen, in line with legal obligations.

Avoiding Tipping-Off

DOUBLED B.V. recognizes that actions such as freezing an account or refusing service could inadvertently signal to the customer that they are under scrutiny. To prevent violations of anti-tipping-off provisions, staff follow strict internal guidelines on how to communicate and act during these sensitive situations. All steps are taken to ensure that enforcement is handled discreetly and in compliance with the law.

Termination of Relationships:

If a player fails to provide sufficient information or engages in suspicious activities, DOUBLED B.V. reserves the right to terminate the relationship. Such decisions are thoroughly documented and approved by senior management.

After termination:

- All related activities are reviewed to ensure compliance.
- Any suspicious transactions are promptly reported to the FIU.
- Records of the terminated relationship are securely retained for at least five years, ensuring availability for regulatory inspections.

8. Suspicious Activity Reporting

DOUBLED B.V. is fully committed to identifying and reporting any activity that may indicate potential money laundering (ML) or terrorist financing (TF). These activities may manifest as irregular or unexpected client behavior, repeated high-value transactions, or interactions with jurisdictions flagged for increased financial crime risk. All employees are expected to remain vigilant and promptly report any observed anomalies to the appointed Compliance Officer. Upon receiving such reports, the Compliance Officer conducts a thorough investigation to determine whether the activity requires further escalation or notification to external authorities.

Recognizing Unusual Transaction Patterns:

Unusual transactions are generally characterized by significant deviations from a customer's known financial behavior or expected activity profile. Such transactions may include unusually large or frequent transfers, dealings with unfamiliar third parties, or operations lacking a clear economic or lawful justification. DOUBLED B.V. utilizes transaction monitoring tools to detect these irregularities and ensure that any red flags are reviewed by the Compliance Officer for further assessment.

In line with applicable regulations, the following types of transactions—whether executed or attempted—are considered unusual and may require detailed review or reporting:

- Transactions Already Reported to Authorities
Any transaction previously flagged and reported to national enforcement agencies, such as the Police or Department of Justice, due to suspected involvement in ML or TF is immediately classified as unusual.
- Transactions Involving Sanctioned Entities or Individuals
Financial activity involving persons or organizations listed under the *Sanctions National Ordinance (N.G. 2014 no. 55)*, or otherwise sanctioned by a competent national body, is regarded as unusual.
- Transactions Equal To or Above NAF 5,000
Regardless of the method—cash, electronic transfer, check, or other—transactions that meet or exceed this threshold are subject to enhanced scrutiny. Examples include:
 - Deposits or withdrawals of NAF 5,000 or more
 - Purchase of gaming chips, tokens, or digital credits totaling NAF 5,000 or more
 - Payouts or prize redemptions equal to or exceeding this value
- Importantly, a single large transaction is not the only trigger—linked or cumulative transactions across a single gaming day that total NAF 5,000 or more are also considered under this classification.
- Transactions Suggestive of ML or TF
Any transaction where there is reason to believe—based on specific indicators or context—that the funds may be tied to money laundering or the financing of terrorism is treated as presumptively unusual and flagged accordingly.

Review and Reporting Protocol:

Once an unusual transaction is reported, the Compliance Officer conducts a detailed evaluation using internal risk criteria and applicable regulatory benchmarks. If the activity is deemed suspicious, a Suspicious Transaction Report (STR) is filed with the Financial Intelligence Unit (FIU) of Curaçao in accordance with national AML guidelines. The decision to report is supported by documented risk analysis and compliance standards.

Confidentiality and Integrity of Reporting:

DOUBLED B.V. enforces a strict confidentiality policy to ensure that the Suspicious Activity Reporting (SAR) process remains secure and compliant. Employees are strictly prohibited from revealing the existence or content of any SAR to the subject of the report or to any unauthorized party. This confidentiality is vital to avoid compromising any active investigation or legal procedure.

All communications relating to SARs must be conducted exclusively with the Compliance Officer or personnel specifically authorized to handle such matters. Any breach of this confidentiality obligation is regarded as a serious infraction of the company's AML policies and may result in disciplinary measures.

By protecting the integrity of the reporting process and ensuring that it is free from interference, DOUBLED B.V. upholds its commitment to regulatory compliance and strengthens its defenses against financial crime.

9. Sanctions

DOUBLED B.V.'s Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) policy emphasizes strict adherence to both national and international sanctions. The company is committed to implementing robust procedures that ensure compliance with sanctions imposed by relevant authorities. These measures are designed to prevent any engagement with sanctioned individuals, entities, or jurisdictions, thereby safeguarding the company's operations and reputation.

Comprehensive Due Diligence:

The cornerstone of the company's sanctions compliance program is the thorough due diligence performed on all clients and transactions. This process ensures that interactions are carefully vetted to avoid breaches of sanctions regulations. Key components include:

- Verifying clients against the latest sanctions lists to identify individuals, entities, or regions subject to restrictions.
- Monitoring transactions to detect any unusual activity that might suggest an attempt to circumvent sanctions.
- Reporting any matches or suspicious activities to the appropriate authorities without delay.

Through a combination of automated systems and manual reviews, DOUBLED B.V. ensures a high level of vigilance in its operations.

Transaction Monitoring and Reporting:

Continuous monitoring is essential to maintaining compliance with sanctions. The company observes all transactions in real time, utilizing automated systems that cross-reference activities against up-to-date sanctions lists. Examples of monitored lists include:

- 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 Nations Security Council Consolidated List
- United Kingdom OFSI Sanctions
- United States OFAC sanctions and List of Foreign Terrorist Organizations

When a potential match or suspicious activity is detected, the following actions are taken:

- Immediate reporting to the Financial Intelligence Unit (FIU) or relevant authorities.
- Freezing of accounts or suspension of transactions to prevent further risk exposure.
- Comprehensive investigations to assess the nature of the detected activity and determine appropriate corrective actions.

Ongoing Staff Training:

DOUBLED B.V. reinforces its commitment to sanctions compliance by providing continuous training to all employees. Staff are educated on:

- The latest updates to sanctions regulations and their application to company operations.
- Techniques for identifying red flags, such as indirect or covert attempts to bypass sanctions.
- Procedures for escalating potential breaches to the Compliance Officer and reporting authorities.

This ensures that personnel remain informed and vigilant, reducing the likelihood of inadvertent violations.

Regular Updates and Audits:

The company's sanctions compliance program undergoes frequent reviews and audits to ensure it aligns with evolving legal requirements and best practices. Regular updates include:

- Enhancements to automated systems to reflect changes in sanctions lists.
- Policy revisions to address emerging risks or new regulatory requirements.
- Independent audits to evaluate the effectiveness of the compliance framework and identify areas for improvement.

Detecting and Addressing Evasion Tactics:

DOUBLED B.V. takes proactive measures to detect and address any attempts to evade sanctions, whether direct or indirect. This includes:

- Identifying patterns of behavior that indicate efforts to bypass restrictions, such as using intermediaries or offshore entities.
- Conducting enhanced due diligence (EDD) on high-risk clients or transactions.
- Reporting suspected evasion tactics to the relevant authorities for further investigation.

Corrective actions are implemented immediately, including the suspension of accounts or transactions and detailed reviews of affected activities.

By integrating rigorous sanctions compliance procedures into its AML/CTF/CPF policy, DOUBLED B.V. ensures it operates within the bounds of international law. This commitment not only mitigates risks but also upholds the company's integrity and trustworthiness within the gaming industry.

10. Compliance Officer

At DOUBLED B.V., a qualified individual is appointed to serve as the Compliance Officer, a cornerstone of the company's Anti-Money Laundering (AML) framework. This appointment is made by senior management to ensure the Compliance Officer possesses the necessary autonomy and authority to oversee the organization's AML program effectively. The selected individual holds substantial expertise in AML compliance and occupies a senior position within the company to ensure they can fulfill their responsibilities with the requisite influence and independence.

The appointment is formalized through an official letter, detailing the Compliance Officer's duties, responsibilities, and reporting structure. This role is integral to the

effective implementation and continuous improvement of the company's AML policies and procedures.

Responsibilities of the Compliance Officer:

The Compliance Officer is entrusted with several critical responsibilities to maintain and enhance the effectiveness of DOUBLED B.V.'s AML program. Their key duties include:

Policy Implementation

The Compliance Officer ensures the effective execution of AML policies and procedures, aligning them with Curaçao's regulatory requirements and international standards.

Central Point of Contact

As the primary point of contact for all AML-related concerns, the Compliance Officer liaises with internal stakeholders, regulatory bodies, and external auditors.

Policy Review and Updates

The Compliance Officer regularly reviews and updates AML policies to address evolving regulatory standards and emerging risks. These updates ensure that the company's AML framework remains robust and compliant.

Training Oversight

The Compliance Officer manages the company's AML training program, ensuring all employees are well-informed about their responsibilities in detecting and reporting suspicious activities. Training materials are frequently updated to reflect legislative changes and industry best practices.

Core Functions of the Compliance Officer:

Transaction Monitoring and Reporting

The Compliance Officer is responsible for analyzing transactions and client activities to identify potential suspicious behavior. They oversee the transaction monitoring systems and ensure the timely filing of Suspicious Activity Reports (SARs) with the Financial Intelligence Unit (FIU). Detailed records of SARs and related internal reports are maintained to meet legal and regulatory requirements.

Policy Development and Adjustment

Crafting and revising AML policies and procedures is a core function of the Compliance Officer. This includes adapting the company's AML framework to

mitigate new risks, address regulatory changes, and implement international best practices.

Employee Training and Awareness

Ensuring that all employees are equipped with the knowledge and skills necessary to detect and report suspicious activities is a primary responsibility. This involves:

- Developing comprehensive training materials.
- Delivering regular training sessions for all employees.
- Updating the training program to align with the latest regulations and company policies.

Regulatory Liaison

The Compliance Officer acts as the principal representative in AML matters when dealing with regulatory bodies, law enforcement agencies, and other authorities. This includes:

- Responding to inquiries or information requests.
- Participating in regulatory inspections and audits.
- Ensuring transparency and cooperation during any compliance reviews.

Compliance Audits

Conducting regular reviews and audits of the company's AML program is a vital function. These audits assess the program's effectiveness, identify areas for improvement, and ensure full compliance with legal requirements. Any deficiencies are promptly addressed through corrective measures.

Record-Keeping

The Compliance Officer maintains detailed and accurate records of all AML-related activities, including:

- Suspicious Activity Reports (SARs).
- Internal reports and transaction reviews.
- Employee training sessions.
- Policy updates and audit findings.

These records are securely stored and made readily accessible for regulatory inspections or audits, as required by Curaçao's AML regulations.

Contribution to Risk Mitigation and Compliance:

By executing these functions, the Compliance Officer plays a pivotal role in safeguarding DOUBLED B.V. against money laundering and terrorist financing risks.

Their work ensures that the company remains compliant with Curaçao's AML regulations while fostering a culture of vigilance and accountability. Through effective oversight, regular updates, and ongoing employee training, the Compliance Officer helps to maintain the integrity of the company's operations and its reputation within the iGaming sector.

11. Senior Management

Senior management at DOUBLED B.V. plays a critical role in overseeing and managing risks associated with Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF). The Board of Directors, in collaboration with the appointed AML/CTF/CPF Officer, ensures that the company maintains a robust compliance framework capable of identifying, mitigating, and addressing financial crime risks effectively.

Oversight and Reporting:

To maintain proper oversight, the Board of Directors requires the AML/CTF/CPF Officer to provide regular updates on significant changes or challenges within the control environment. These updates include:

- Monthly risk assessments, identifying potential vulnerabilities in internal controls.
- An annual report that evaluates the effectiveness of the company's AML/CTF/CPF measures, policies, and procedures.

If deficiencies or gaps are identified, the AML/CTF/CPF Officer collaborates with senior management to propose and implement corrective measures. These recommendations are presented to the Board for approval, ensuring that the company's risk management efforts are continuously strengthened.

Policy and Procedure Reviews:

Senior management is responsible for conducting comprehensive reviews of all AML/CTF/CPF policies and procedures at least once annually. These reviews are informed by insights gained from monthly risk assessments and operational feedback, allowing the company to address weaknesses proactively.

Key responsibilities include:

- Evaluating the effectiveness of existing policies in mitigating identified risks.

- Approving updates or modifications to align with evolving regulatory requirements and emerging threats.
- Ensuring that risk management practices are responsive to changes in the regulatory landscape or the company's operational environment.

Employee Training and Awareness:

DOUBLED B.V. recognizes that employees are on the front line of its AML/CTF/CPF compliance efforts. As such, senior management oversees the development and implementation of comprehensive training programs designed to enhance employee awareness and capability in managing financial crime risks.

The training programs focus on:

- Educating employees about the types of AML/CTF/CPF risks relevant to their roles.
- Ensuring that staff can identify and escalate suspicious activities effectively.
- Providing regular updates on changes to legislation or internal policies to ensure all employees remain informed and compliant.

Specialized training is provided to employees in high-risk or critical roles to ensure they have the expertise required to manage complex compliance challenges.

Strengthening the Internal Control Framework:

Senior management ensures that the company's internal control framework is robust and aligned with industry best practices. This framework includes:

- Adequate segregation of duties to minimize the risk of conflicts of interest or internal fraud.
- Clear authorization processes to ensure that all transactions and activities are properly approved.
- Ongoing monitoring of transactions and operations to identify and address anomalies in real time.
- Thorough documentation of all compliance-related activities, providing a reliable audit trail for regulatory inspections.

These controls are designed to provide a solid foundation for the company's compliance efforts and to minimize the risks associated with financial crime.

Independent Audits and Assessments:

To ensure objectivity and continuous improvement, senior management facilitates regular independent audits and assessments of the AML/CTF/CPF program. These evaluations provide:

- An unbiased assessment of the program's effectiveness and alignment with regulatory requirements.
- Insights into areas for improvement in policies, procedures, and operational controls.
- Assurance to stakeholders and regulators that the company is committed to maintaining the highest standards of compliance.

Recommendations from these audits are reviewed and acted upon by senior management to enhance the overall effectiveness of the compliance program.

Commitment to Compliance and Risk Mitigation:

Through their oversight and strategic direction, senior management ensures that DOUBLED B.V. remains committed to mitigating money laundering, terrorism financing, and proliferation financing risks. Their leadership in implementing robust policies, fostering a culture of compliance, and responding proactively to emerging risks underscores the company's dedication to regulatory excellence and operational integrity.

By maintaining a dynamic and responsive compliance framework, senior management upholds the integrity of the company's operations and protects its reputation within the iGaming industry.

12. Training & Record Keeping

DOUBLED B.V. has developed a comprehensive training program and robust record-keeping protocols to ensure compliance with its Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) obligations. These efforts are integral to equipping employees with the knowledge and tools needed to detect and prevent financial crimes while maintaining regulatory compliance and operational integrity.

AML/CTF/CPF Training Program:

The company's AML/CTF/CPF training program is designed to provide employees with essential knowledge about identifying and mitigating risks related to money laundering, terrorism financing, and proliferation financing. By fostering an informed workforce, DOUBLED B.V. ensures the effective application of its compliance policies, thereby supporting the integrity and credibility of the iGaming sector.

Objectives of the Training Program

- Educate employees on their legal obligations under Curaçao's AML/CTF/CPF regulations.
- Enhance the ability to identify suspicious behaviors and financial activities.
- Familiarize staff with internal procedures for customer identification, verification (KYC/CDD), and reporting suspicious activities.
- Raise awareness of record-keeping requirements and the consequences of non-compliance.
- Highlight emerging trends and techniques in money laundering and terrorism financing.

Tailored Training for Roles

The training program is mandatory for all employees, with content tailored to the specific responsibilities and risk exposure of each role. Participants include:

- Senior management and compliance officers.
- Customer-facing personnel.
- Operational and back-office staff involved in financial transactions.
- Employees in roles with heightened exposure to AML/CTF/CPF risks.

Delivery and Frequency

New hires receive comprehensive training upon joining the company, while all employees participate in annual refresher courses. For roles involving greater exposure to compliance risks, additional training sessions may be conducted more frequently.

Training is delivered using a variety of methods to cater to different learning styles and reinforce key concepts, including:

- In-person workshops and seminars.
- Interactive e-learning modules and online courses.
- Practical exercises, such as case studies and role-playing scenarios.

Training Content

The program covers critical topics, including:

- Curaçao-specific AML/CTF/CPF laws and regulations.
- Internal company policies and procedures.
- Customer identification and verification processes (KYC/CDD).
- Techniques for detecting and reporting suspicious activities.
- Record-keeping obligations and best practices.
- Emerging threats and trends in financial crimes.

Training sessions are led by qualified professionals, such as internal compliance officers or external consultants, who bring up-to-date expertise and insights into the latest legal and industry developments.

Record-Keeping Standards:

DOUBLED B.V. adheres to stringent record-keeping practices to meet regulatory standards and support its AML/CTF/CPF compliance efforts. These practices ensure the secure and efficient management of critical documentation.

Retention of Records

The company retains the following records for a minimum of five years, as required by Curaçao regulations:

- Customer identification information (e.g., KYC data).
- Transaction records and histories.
- Suspicious Activity Reports (SARs) and related documentation.
- Training attendance logs and materials.
- Internal and external audit findings.

Data Security

All records are protected with robust encryption protocols and access controls to prevent unauthorized access or tampering. Key measures include:

- Regular security audits to ensure data integrity and compliance with legal standards.
- Multi-level access controls to restrict data availability to authorized personnel only.
- Secure storage systems that prevent breaches and unauthorized modifications.

Efficient Retrieval and Monitoring

The company employs a systematic organization of records to enable swift retrieval when needed by authorized staff or regulatory bodies. Continuous internal monitoring ensures that records are maintained properly, and periodic audits confirm their accuracy and accessibility.

Supporting Compliance and Auditing

By managing records effectively, DOUBLED B.V. ensures compliance with Curaçao's AML/CTF/CPF requirements and facilitates smooth auditing processes. These efforts bolster the company's reputation for integrity and reliability within the gaming industry.

Through its robust training initiatives and meticulous record-keeping practices, DOUBLED B.V. demonstrates its commitment to mitigating financial crime risks while maintaining compliance with regulatory obligations and supporting industry-wide best practices.

13. AML/CTF/CPF Audit

To comply with Curaçao's updated gaming regulations, DOUBLED B.V. undergoes an independent annual audit focused on Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF). This audit serves as a critical tool to evaluate the effectiveness of the company's compliance measures, ensuring alignment with legal standards and industry best practices while mitigating financial crime risks.

Objectives of the AML/CTF/CPF Audit:

The primary goal of the audit is to assess the company's AML/CTF/CPF framework, identify potential deficiencies, and recommend corrective actions. By conducting regular audits, DOUBLED B.V. ensures its policies, procedures, and practices remain robust, compliant, and capable of addressing evolving risks.

The audit evaluates key areas, including:

- Risk assessments and their implementation.
- Transaction monitoring systems and reporting mechanisms.
- Employee training programs on AML/CTF/CPF compliance.
- KYC (Know Your Customer), KYB (Know Your Business), and CDD (Customer Due Diligence) protocols.
- Overall compliance with Curaçao's gaming regulations and international AML/CTF/CPF standards.

Role of the Independent Auditor:

DOUBLED B.V. engages a qualified external auditor or an internal audit team with specialized AML/CTF/CPF expertise. The auditor is independent of the company's AML Compliance team to ensure objectivity and avoid conflicts of interest. The chosen auditor's qualifications, credentials, and industry reputation are carefully evaluated, and approval is sought from the Gaming Control Board (GCB), as required by Curaçao regulations.

Key responsibilities of the independent auditor include:

- Conducting a comprehensive review of the company's AML/CTF/CPF framework.
- Identifying weaknesses or gaps in compliance measures.
- Providing actionable recommendations to strengthen the company's controls.

The audit process adheres to international standards and specific requirements outlined by the GCB.

Audit Process:

The audit involves a thorough examination of the company's AML/CTF/CPF practices across various domains:

1. Evaluation of AML/CTF/CPF Policies and Procedures
 - Determine whether policies are current and comply with Curaçao regulations.
 - Assess how effectively policies are implemented across the organization.
2. Risk Management Assessment
 - Review the company's risk assessment processes and mitigation strategies.
 - Ensure risks related to high-risk jurisdictions, PEPs (Politically Exposed Persons), and transaction types are effectively addressed.
3. Transaction Monitoring Review
 - Analyze the efficiency of systems for detecting and reporting suspicious activities.
 - Evaluate alert thresholds and system capabilities.
4. Staff Training Evaluation
 - Assess the adequacy and frequency of employee training programs.
 - Verify that training content aligns with current legal requirements and industry practices.
5. Reporting Mechanism Audit
 - Examine the company's procedures for reporting suspicious transactions to the Financial Intelligence Unit (FIU).
 - Review the timeliness and accuracy of Suspicious Activity Reports (SARs).
6. Customer File Review
 - Verify compliance with KYC, KYB, and CDD protocols.
 - Assess the completeness and accuracy of customer records.

Audit Findings and Reporting:

Following the audit, the independent auditor delivers a detailed report to DOUBLED B.V.'s senior management and the Gaming Control Board. The report includes:

- An overview of the audit scope and methodology.
- Identified deficiencies or compliance gaps.
- Recommendations for corrective actions and improvements.

The company is required to address these recommendations within a specified timeframe. In cases where significant issues are identified, follow-up audits may be conducted to ensure corrective measures are effectively implemented.

Oversight by the Gaming Control Board:

The Gaming Control Board (GCB) plays a central role in overseeing the company's AML/CTF/CPF compliance efforts. In addition to reviewing audit reports, the GCB may:

- Conduct onsite inspections to verify audit findings and assess the implementation of corrective actions.
- Interview relevant staff and analyze documentation to gain a comprehensive understanding of the company's practices.
- Request additional documents or perform targeted evaluations of specific compliance areas.

If the GCB identifies non-compliance during its review or inspections, the company may face penalties ranging from fines and operational restrictions to suspension or revocation of its gaming license.

Commitment to Corrective Actions:

DOUBLED B.V. is committed to promptly addressing any deficiencies identified during the audit process. The company works closely with the GCB to ensure corrective measures are implemented effectively and regulatory compliance is maintained. Steps taken include:

- Revising and updating AML/CTF/CPF policies and procedures.
- Strengthening internal controls and monitoring systems.
- Conducting follow-up training for employees to address identified gaps.

By demonstrating a proactive approach to compliance, DOUBLED B.V. reinforces its dedication to mitigating risks and maintaining the integrity of its operations.

The Importance of AML/CTF/CPF Audits:

Regular independent audits ensure that DOUBLED B.V. remains aligned with Curaçao's gaming regulations and international AML/CTF/CPF standards. These

audits not only safeguard the company's reputation but also contribute to the broader effort to combat financial crimes in the iGaming sector.

Through its commitment to transparent and rigorous compliance practices, DOUBLED B.V. upholds the highest standards of accountability and operational excellence.

14. Abbreviations & Definitions

Alert

An automated or manual notification triggered by predefined criteria or anomalies, signaling the need for further investigation into potential suspicious activity or financial crime.

Anti-Money Laundering (AML)

A system of internal policies and procedures designed to prevent and detect the concealment of funds derived from illegal activity. AML measures form part of the broader compliance obligations of DOUBLED B.V.

AML Policy

The Company's documented framework outlining its commitment to combat money laundering and terrorism financing. The policy includes internal controls, responsibilities, and reporting procedures, led by the Money Laundering Reporting Officer (MLRO) and subject to internal audits.

AML/CTF/CPF Program

An integrated approach to preventing money laundering, terrorist financing, and proliferation financing, encompassing all internal policies, procedures, monitoring systems, and training initiatives under the supervision of the MLRO.

Beneficial Owner

The individual who ultimately owns or controls a customer account, even if the account is formally held by another party.

Blacklist

A database of persons, entities, or jurisdictions identified as posing a compliance risk, often due to sanctions or regulatory violations. Blacklists are used to restrict or block transactions.

Board of Directors (BoD)

The governing body responsible for overseeing DOUBLED B.V.'s operations, including compliance, risk management, and strategic planning.

Comprehensive Sanctions

Broad economic or trade restrictions imposed by governments or international bodies against countries, entities, or individuals, usually with minimal exceptions.

Counter-Proliferation Financing (CPF)

Efforts to prevent the flow of funds used to support the development and distribution of weapons of mass destruction.

Counter-Terrorism Financing (CTF)

Initiatives aimed at detecting and stopping financial transactions that support terrorism or related activities.

Criminal Proceeds

Assets or income derived, directly or indirectly, from criminal conduct.

Customer

An individual or legal entity that enters into a business relationship with DOUBLED B.V., including account registration or participation in its services.

Customer Due Diligence (CDD)

A process of verifying a customer's identity and evaluating their risk profile. It serves as the foundation for compliance with AML/CTF laws and helps in detecting suspicious conduct.

Customer Relationship

The ongoing interaction between DOUBLED B.V. and a customer, beginning from onboarding and continuing through the lifecycle of account activity and service usage.

Due Diligence

A set of checks and evaluations conducted to assess the legal, financial, and reputational risks associated with a customer or business relationship.

Economic Sanctions

Measures imposed by national or international bodies restricting financial or trade activities with designated individuals, entities, or countries.

Egmont Group of FIUs

A global organization that supports cooperation and information exchange between national Financial Intelligence Units to strengthen AML and CTF efforts.

Embargo

A government-imposed ban on trade or financial dealings with a specific country or group.

Enhanced Due Diligence (EDD)

A deeper level of customer verification required for individuals or entities assessed as posing higher financial crime risk.

European Union (EU)

A political and economic bloc of European countries that issues regulatory directives and sanctions lists affecting AML/CTF enforcement.

Exclusions List

A list maintained by compliance personnel to identify names or entities that have been cleared after initial screening and no longer require monitoring.

Financial Action Task Force (FATF)

An international standard-setting body that promotes global efforts to combat money laundering and terrorist financing. FATF publishes country assessments and high-risk jurisdiction lists.

Financial Intelligence Unit (FIU)

A government agency designated to receive, analyze, and refer suspicious financial activity reports to law enforcement or regulatory bodies. In Curaçao, this is the FIU-Curaçao.

First Line of Defense

Front-line employees who collect and verify customer information, conduct onboarding, and serve as the initial gatekeepers for AML/CTF controls.

Greylist

A compilation of countries or regions that are found to have strategic AML/CTF deficiencies but are working toward remediation.

High-Risk Third Country

A country identified by international authorities (e.g., FATF, EU) as lacking sufficient measures to prevent ML or TF and therefore requiring enhanced scrutiny.

Inherent Risk

The level of risk associated with a customer, product, or transaction before any mitigating controls are applied.

Investigation

The formal process of reviewing and assessing information related to potential financial crime, policy breaches, or regulatory violations.

Know Your Business (KYB)

A due diligence process focused on verifying the structure, ownership, and legitimacy of corporate clients or business partners.

Know Your Customer (KYC)

A fundamental compliance process used to confirm customer identities and understand their financial behavior, enabling risk assessment and transaction monitoring.

Know Your Employee (KYE)

Internal controls designed to assess employee integrity and detect potential internal threats, such as conflicts of interest or criminal backgrounds.

Layering

A stage in the money laundering process where illicit funds are moved through multiple transactions to obscure their origin.

Minor

Any individual under the age of 18.

Monitoring

The continuous review of customer behavior and transaction patterns, supported by automated systems, to identify and report suspicious activities.

Money Laundering

The process of disguising illegally obtained money through a series of transactions intended to make it appear legitimate. It typically includes three stages: placement, layering, and integration.

Money Laundering Reporting Officer (MLRO)

The designated individual responsible for implementing AML/CTF policies, reviewing internal alerts, and filing Suspicious Transaction Reports (STRs) to the appropriate authorities.

National Ordinance on Offshore Games of Hazard (NOOGH)

The legislation governing offshore gaming operations in Curaçao, which includes provisions related to AML/CTF compliance.

Office of Foreign Assets Control (OFAC)

A department of the U.S. Treasury that administers and enforces economic sanctions programs targeting foreign threats.

PEP – Politically Exposed Person

A person entrusted with a prominent public function whose position presents potential exposure to corruption and thus requires enhanced scrutiny.

Red Flag

A signal or indication that a transaction or behavior may be suspicious and warrants additional review or investigation.

Regulatory Agency

A governmental authority responsible for enforcing financial regulations and overseeing compliance obligations of licensed entities.

Sanctions List (Mandatory)

Official databases—such as those from the UN, OFAC, or EU—that organizations are legally required to screen when conducting transactions or onboarding customers.

SAR/STR – Suspicious Activity/Transaction Report

A formal submission to the Financial Intelligence Unit (FIU) when a transaction or behavior is suspected to be linked to money laundering or terrorist financing.

Source of Funds / Source of Wealth (SOF/SOW)

Information provided by the customer to clarify where their assets or income originate, used to validate legitimacy and assess risk.

UK – United Kingdom

A jurisdiction with its own AML/CTF framework and regulatory expectations, often referenced in global compliance.

UN – United Nations

An intergovernmental organization whose Security Council issues sanctions lists that member countries are required to enforce.

US – United States

A jurisdiction with robust AML/CTF enforcement mechanisms and global influence in financial regulatory practices.