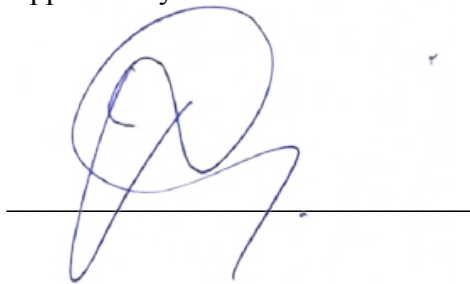


ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING POLICY

Prevailer B.V.

28/05/2025

Approved by the Board of Directors

A handwritten signature in blue ink, consisting of a large, stylized 'A' followed by a series of loops and a long horizontal stroke, is written over a solid black horizontal line.

Next Review: May 2026

Responsible Compliance Officer:

Abdulrasaq Folorunsho

compliance@prevailer.com

TABLE OF CONTENTS

- 1. Definitions**
- 2. Policy**
- 3. iGaming Environment**
- 4. Money Laundering, Terrorism Financing & Proliferation Financing**
- 5. Risk Assessment**
- 6. Customer Due Diligence**
- 7. Sanctions Compliance**
- 8. Management Responsibilities**
- 9. Compliance Officer**
- 10. Suspicious Activities**
- 11. Audit Procedures**
- 12. Record Keeping**
- 13. Training**



1. DEFINITIONS

Key Abbreviations

- **AML (Anti-Money Laundering):** Preventing the concealment of illicitly obtained funds to make them appear legitimate.
- **CTF (Counter Terrorism Financing):** Measures to combat the financial support of terrorist activities.
- **CPF (Counter Proliferation Financing):** Strategies to prevent funding for the proliferation of weapons of mass destruction.
- **EDD (Enhanced Due Diligence):** In-depth checks applied to higher-risk customers to mitigate potential risks.
- **CDD (Customer Due Diligence):** Verification processes to confirm customer identity and assess risks like money laundering.
- **FIU (Financial Intelligence Unit Curaçao):** National agency analyzing and forwarding suspicious transaction reports as per the Norut.
- **KYC (Know Your Customer):** Procedures to verify a customer's identity and understand their typical activity.
- **KYB (Know Your Business):** Verification of a business's legitimacy, including its directors and operations.
- **SAR/STR (Suspicious Activity Report/Suspicious Transaction Report):** Reports submitted for irregular activities indicating potential illicit behavior.
- **SOF/SOW (Source of Funds/Wealth):** Identification of the origin of funds or assets.
- **PEP (Politically Exposed Person):** Individuals in prominent public positions, subject to additional due diligence.
- **UBO (Ultimate Beneficial Owner):** The individual ultimately controlling or benefiting from a company or transaction.

Governance and Oversight

- **BoD (Board of Directors):** The company's governing body responsible for strategic decisions.
- **Compliance Officer:** A senior management role responsible for ensuring the company complies with AML/CFT regulations, independent of operational activities.
- **Money Laundering Reporting Officer (MLRO):** Oversees AML activities, suspicious transaction reporting, and program audits.



International Organizations

- **FATF (Financial Action Task Force):** Sets global AML standards and evaluates country compliance.
- **CFATF (Caribbean Financial Action Task Force):** Regional AML organization for the Caribbean Basin and Central/South America.
- **Egmont Group:** International network of FIUs promoting collaboration and expertise exchange to combat financial crimes.
- **OFAC (Office of Foreign Assets Control):** US Treasury Department managing economic sanctions and the SDN list.
- **United Nations (UN):** Global organization combatting crime and terrorism financing through initiatives like GPML.
- **European Union (EU):** Economic and political union with robust AML/CFT directives.
- **UK (United Kingdom) & US (United States):** Jurisdictions enforcing stringent AML/CFT standards.

Sanctions and Risk Management

- **Blacklist:** Internal and official lists screening names/entities for sanctions exposure.
- **Sanctions List:** Database of individuals/entities prohibited from business interactions.
- **Sanctions Compliance:** Adherence to laws regarding trade, financial restrictions, and movement.
- **Red Flag:** Indicators of potentially suspicious transactions or activities.
- **High-Risk Third Country:** Nations with significant AML deficiencies identified by FATF.
- **Risk-Based Approach:** Tailored AML measures based on client and transaction risks.

AML Concepts

- **Money Laundering:** Concealing illicit funds through placement, layering, and integration.
- **AML Policy:** Internal framework to prevent money laundering and terrorist financing, led by an AML compliance team.
- **Anti-Money Laundering and Counter-Financing of Terrorism Program:** Strategies to mitigate financial crime risks, including training and audits.

- **Structuring:** Splitting transactions to evade detection or reporting requirements.

Tools and Processes

- **Automated Screening Tool (AST):** Software for customer and sanctions screening.
- **Exclusions List:** Names verified by compliance as unrelated to sanctions matches.
- **Simple Checks:** Initial review of flagged alerts to determine further action.
- **Investigation:** Detailed analysis of potential sanctions violations.
- **Monitoring:** Ongoing review of customer activities for irregular patterns.

Local Context: Curaçao

- **NOOGH (National Ordinance on Offshore Games of Hazard):** Regulatory framework for offshore gaming operations.
- **The Curaçao Gaming Control Board (GCB):** Supervisory authority for AML/CFT compliance in gaming.

2. POLICY

Prevailer B.V (“the Company”) is dedicated to preventing money laundering and the financing of terrorism through the establishment of this comprehensive Policy. This policy is aligned with both local and international standards to ensure compliance with all relevant regulations.

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

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

The Policy adheres to key legislation in Curacao, which includes the National Ordinance for Games of Chance (LOK), the Criminal Code of Curacao, the National Ordinance on Offshore Games of Hazard (NOOGH), the National Ordinance Penalization of Money Laundering (NOPML), the National Ordinance on the Reporting of Unusual Transactions (NORUT), and the National Ordinance on Identification when Rendering Services (NOIS), effective from May 16,

2024. The policy also complies with the Sanctions National Ordinance (SNO) and the Kingdom Sanction Act.

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

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

3. iGAMING ENVIRONMENT

Prevailer B.V. is a private company with a statutory seat at Willemstad, Curacao, and its address at Chuchubiweg 17. Registered in the Curacao Commercial Registry under number 149548. Prevailer B.V. is licensed by the Curaçao Gaming Authority to offer games of chance under license number OGL/2024/341/0759. Consequently, the Company focuses its operations exclusively in markets where online gambling is permitted by law and refrains from targeting customers in regions where it is not allowed.

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

4. MONEY LAUNDERING, TERRORISM FINANCING & PROLIFERATION FINANCING

Money Laundering

Money laundering remains one of the most significant enablers of global financial crime. It involves concealing the origins of criminally derived funds and integrating them into the legitimate financial system. This process often spans multiple jurisdictions and supports a variety of illegal activities, including corruption, drug trafficking, tax evasion, smuggling, and sanctions evasion. At its core, money laundering is designed to obscure the identity, source, and destination of illicit proceeds, allowing criminals to benefit from their crimes without detection.

The laundering process generally unfolds in three stages: placement, layering, and integration. During the placement stage, illegally obtained funds are introduced into the financial system. This is often achieved through deposits into bank accounts, the purchase of high-value items, or by using gambling platforms. Layering then involves a series of complex transactions aimed at disguising the trail—transferring money between accounts, changing currencies, or investing in

assets to break the audit trail. Finally, integration is where the laundered money is absorbed into the legitimate economy, often through investments, luxury purchases, or business ventures.

Online gambling platforms are especially vulnerable to abuse due to their digital nature, high transaction volume, and borderless operations. Prevailer B.V. takes this risk seriously and mitigates it by disallowing anonymous participation and maintaining strict oversight of customer activity and transaction behavior.

Though terrorist financing differs in motivation, the mechanics used to disguise and move funds often mirror those of money laundering. Whether funds originate from legal sources like donations or illegal activities such as trafficking or extortion, they are typically funneled through similar laundering techniques. A common method involves the use of prepaid cards to maintain anonymity and fund logistics discreetly. Prevailer B.V. ensures that its staff remains well-informed of such methods and regularly trained to detect and report suspicious activity tied to both money laundering and terrorist financing.

To address these risks, Prevailer B.V. adopts a comprehensive risk management strategy. Customer identity is rigorously verified through robust due diligence measures that include the confirmation of age, location, and identification documents. Politically Exposed Persons (PEPs) and other high-risk customers are subject to Enhanced Due Diligence (EDD). Transactions are continuously monitored for irregularities, including unusual volumes, frequent activity, and the use of multiple accounts. Any attempt to use the platform as a pass-through or temporary repository for illicit funds is flagged and investigated. The company also controls peer-to-peer functionality to prevent its misuse for hidden transfers. Staff are routinely trained on these protocols, and risk assessments are updated regularly to reflect the evolving threat landscape.

Terrorist Financing

Terrorist financing refers to the collection or provision of funds intended to support terrorist operations, ranging from minor tactical missions to large-scale attacks. These funds are essential for planning, recruiting, training, acquiring materials, and executing operations. What makes terrorist financing particularly difficult to detect is the diversity of its sources. Funding may come from both legal activities, such as charitable donations and business revenues, and illegal ones, such as drug trafficking, smuggling, or fraud. This duality allows terrorist groups to operate under the radar, especially when legitimate transactions are exploited to disguise illicit intent.

Prevailer B.V. understands that the challenge lies not only in identifying illegal activity but also in discerning when legitimate financial channels are being misused. For instance, charities and nonprofit organizations can be manipulated to divert donor funds to terrorist causes. Similarly, businesses may act as fronts to funnel money under the appearance of normal commercial operations.

The transfer of terrorist funds occurs through both formal and informal systems. Formal systems involve traditional banks, online payment processors, and financial institutions, where layering and structuring may be employed to disguise the source and destination of funds. Informal systems, such as hawala and other trust-based remittance networks, bypass conventional oversight and often leave little to no documentation, making them difficult to trace.

To counter these threats, Prevailer B.V. monitors for red flags, including high-frequency transfers to or from conflict zones, links to known terrorist entities, and suspicious activity in sectors such as charity, where abuse is more likely. Financial behavior that lacks economic logic or is structured to evade thresholds is closely scrutinized.

The company's AML policies are designed to detect and prevent terrorist financing by ensuring that customer verification processes are rigorous, and that all transactions are subject to automated monitoring systems. Additional scrutiny is applied to high-risk accounts, and the company screens all customers and counterparties against multiple sanctions lists. These include the Sanctions National Ordinance, Kingdom Sanction Act, the OFAC SDN list, and international lists maintained by the UN, EU, and U.S. State Department.

Prevailer B.V. aligns its practices with global frameworks such as the Financial Action Task Force (FATF) recommendations, OFAC's enforcement guidelines, EU directives, and United Nations resolutions. These efforts are supported by ongoing staff training and regular compliance reviews, ensuring that the company remains equipped to detect, prevent, and respond to evolving threats of terrorist financing.

Proliferation Financing

Proliferation Financing (PF) refers to the use of financial resources to support the development, manufacture, or distribution of weapons of mass destruction (WMD), including their delivery systems. Recognizing the severe global security risks posed by PF, Prevailer B.V. is committed to preventing its platform from being used, even indirectly, to facilitate such activity.

The company takes a proactive approach by embedding PF-specific controls into its AML compliance framework. These include enhanced risk assessments focused on jurisdictions and customer profiles associated with proliferation risk. Where elevated risk is identified, Enhanced Due Diligence is applied to verify the legitimacy of both the customer and the financial activity in question.

Prevailer B.V. strictly adheres to the sanctions regimes issued by the United Nations Security Council, the European Union, the Sanctions National Ordinance, and the Kingdom Sanction Act. All transactions are screened against relevant sanctions lists to ensure no dealings occur with entities or individuals linked to WMD proliferation. By maintaining this level of diligence, the company supports international non-proliferation efforts and safeguards the integrity of its operations.

5. RISK ASSESSMENT

At Prevailer B.V., the foundation of our compliance program lies in a structured and ongoing risk-based approach (RBA), through which we systematically identify, assess, and mitigate financial crime risks across all areas of operation. This framework ensures that we remain vigilant against the threats of money laundering (ML), terrorist financing (TF), and proliferation

financing (PF), while maintaining compliance with Curaçao's regulatory obligations and global best practices.

Risk Assessment Methodology

Our risk assessment process is multi-dimensional, focusing on key areas such as customer behavior, products and services, transaction types, geographic exposure, and distribution channels. By regularly reviewing each of these areas, Prevailor B.V. remains equipped to detect vulnerabilities and implement timely, proportionate countermeasures. Special attention is given to individuals with higher-risk profiles, complex financial arrangements, or links to jurisdictions with limited AML/CTF/CPF oversight.

Customer-related risk assessments consider a variety of factors, including whether individuals are classified as politically exposed persons (PEPs), originate from high-risk regions, or are connected to opaque or layered ownership structures. In such cases, Enhanced Due Diligence (EDD) procedures are deployed, which may include in-depth verification of identity, review of source of funds, and continuous profile monitoring. Customers exhibiting erratic or disproportionate gambling behavior are also flagged for heightened scrutiny.

Products and services offered by Prevailor B.V. are evaluated to determine their inherent risk of misuse. Services that allow for high-value or anonymous transactions, or those that facilitate fund transfers without corresponding gambling activity, are subject to stricter oversight. The use of prepaid cards, virtual currencies, or third-party financial tools are particularly scrutinized due to their limited transparency. The company also monitors for the misuse of player accounts as financial conduits, as well as peer-to-peer functionality that could enable fund movement outside the intended gaming context.

Geographical risk is another critical element. Prevailor B.V. maintains a continuously updated country risk matrix informed by sources such as FATF publications, CFATF regional alerts, the U.S. Department of State's INCSR, Transparency International's Corruption Perceptions Index, and relevant EU and OFAC sanctions lists. Based on this intelligence, jurisdictions are classified by risk level, with customers from high-risk countries subject to enhanced vetting, additional monitoring, and restricted service availability when appropriate.

Our approach also includes evaluating the risk associated with distribution channels. The company acknowledges the vulnerabilities posed by non-face-to-face interactions and digital environments where anonymity can be exploited. To mitigate these risks, Prevailor B.V. has embedded advanced identity verification tools across all customer access points. This includes digital KYC solutions, biometric checks, and robust authentication procedures. Furthermore, no transactions or customer engagements are permitted through unregulated or unidentified third parties, and all business relationships must originate through secure, traceable channels.

Sector-Specific Risks in iGaming

Given the specific vulnerabilities within the online gambling industry, Prevailor B.V. has tailored its compliance controls to meet the challenges unique to the sector. Gambling platforms can be exploited to obscure the origin of funds, particularly through layered betting patterns, rapid fund

turnover, and irregular payout behaviors. Criminals may use these tactics to convert illicit funds into seemingly legitimate winnings.

To counteract this, the company ensures that all deposits and withdrawals are routed exclusively through licensed financial institutions. Payments using anonymous or untraceable instruments, such as certain cryptocurrencies or unregistered prepaid cards, are restricted or entirely prohibited. Monitoring tools have been configured to detect unusual betting patterns, excessive deposit frequency, and sudden withdrawals that deviate from typical gaming behavior.

Employee training plays a vital role in strengthening the company's overall risk posture. Compliance staff and customer-facing teams are routinely trained to recognize red flags, report suspicious activity, and stay informed of evolving criminal methodologies within the gambling landscape.

Mitigation Measures

When a risk is identified—whether at the customer, transaction, jurisdictional, or service level—Prevailer B.V. responds with tailored mitigation strategies. EDD is applied to higher-risk profiles, requiring additional documentation and background checks. The company collects detailed information on the source and intended use of funds, while conducting ongoing screenings against global sanctions lists and watchlists.

Sophisticated transaction monitoring systems operate continuously in the background, equipped with real-time alerting capabilities. These systems analyze transaction flow and behavior to detect anomalies, flagging them for internal review. Alerts generated are triaged and, when necessary, escalated for formal investigation and reporting to the Financial Intelligence Unit (FIU).

To protect against identity fraud, strict verification processes are enforced. These include cross-referencing customer data against sanctions databases, screening for duplicate accounts, and performing regular updates to maintain the accuracy of stored information.

Monitoring, Policy Adaptation and Reporting

Prevailer B.V. understands that financial crime risks are dynamic, requiring constant vigilance. To ensure our controls remain effective, we conduct periodic internal reviews of transaction activity, customer risk ratings, and compliance procedures. These findings inform policy updates and the adaptation of monitoring tools, ensuring alignment with both regulatory changes and emerging criminal tactics.

All suspicious transactions are promptly reported to the appropriate authorities in accordance with regulatory obligations. Record-keeping is maintained at a high standard—covering customer onboarding details, transaction data, risk classification documentation, and due diligence records—for the required legal retention period. These records are securely stored and made available for inspection during audits or regulatory reviews, reflecting the company's commitment to transparency and accountability.

Integrated Risk Governance

Through this holistic and risk-focused compliance strategy, Prevailer B.V. demonstrates its commitment to preventing financial crime within the iGaming sector. By integrating compliance into every level of operations—from onboarding to transaction oversight—the company ensures that it not only complies with Curaçao’s AML/CTF/CPF requirements but also contributes to the integrity and trustworthiness of the broader financial system.

Technological Developments Risk Assessment

Prevailer B.V. acknowledges that rapid technological evolution in the iGaming space brings both opportunities and risks. To prevent financial crime from taking advantage of emerging tools, the company incorporates technology-specific risk assessments into its compliance framework. Each new product, service, or platform enhancement is reviewed in advance to determine whether it introduces any new vulnerabilities.

Risk assessments are triggered by the introduction of new business models, payment systems, account access features, or backend technologies—such as blockchain, artificial intelligence, or cybersecurity enhancements. Before deployment, the company evaluates each innovation for potential misuse and documents all findings in line with AML/CTF best practices. These records not only help ensure internal accountability but also support regulatory review.

If risks are identified, Prevailer B.V. implements tailored countermeasures. These may include reinforcing authentication processes with MFA or biometrics, encrypting data streams, or enhancing transaction monitoring capabilities with AI-based analytics. Monitoring systems are configured to detect subtle behavioral deviations and to respond dynamically to new fraud typologies.

Compliance policies are updated continuously to align with these technological shifts. Prevailer B.V. ensures that its internal controls evolve in tandem with both operational innovations and emerging financial crime trends. This proactive approach ensures the platform remains resilient and compliant without compromising on innovation or user experience.

Through vigilant evaluation and integration of technology controls, Prevailer B.V. upholds a secure, adaptable, and forward-thinking compliance environment. This commitment ensures that regulatory requirements are not only met but exceeded, and that the company remains a trusted operator in the global iGaming industry.

6. CUSTOMER DUE DILIGENCE

The company is dedicated to maintaining compliance with regulatory standards that prohibit the establishment of anonymous or fictitious accounts within the casino sector. To effectively combat risks related to money laundering, terrorist financing, and proliferation, it is imperative to verify player identities and comprehend their business relationships. A comprehensive Customer Due Diligence (CDD) policy is essential for evaluating risks and ensuring adherence

to all regulatory obligations. Any activities deemed suspicious will be reported to the Financial Intelligence Unit (FIU) and, if necessary, to the Public Prosecutor's Office.

The company will implement CDD measures under the following conditions:

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

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

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

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

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

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

- **Risk Evaluation:** Players will be assigned initial risk ratings based on collected information, which will be revised as more data becomes available to determine the appropriate level of CDD.
- **Verification Methods:** Identity verification will be executed through:



- Government-issued photo identification (e.g., passport or ID card).
- Supplementary documents (e.g., utility bills or bank statements) confirming the address, dated within the last six months.
- Verification of the address through communication methods such as letters, email, or phone.
- Biometric checks, cross-referencing database information, IP addresses, and funding methods.

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

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

Timing of Customer Due Diligence Measures

Prevailer B.V. enforces the timely implementation of Customer Due Diligence (CDD) procedures to ensure full compliance with applicable Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulations. These procedures are designed to proactively identify and verify customers in accordance with regulatory requirements and internal risk assessments.

CDD Triggered by Transaction Thresholds

At the point of account registration, Prevailer B.V. collects and verifies core customer information, including full legal name, permanent residential address, and date of birth. Additionally, customers undergo Politically Exposed Person (PEP) screening and are cross-checked against relevant sanctions lists to ensure they are not linked to prohibited or high-risk entities.

In line with the company's risk-based approach, full identity verification is completed prior to processing any financial transaction that reaches or exceeds the threshold of NAF 4,000. This requirement applies to both individual transactions and cumulative transactions—such as multiple deposits, withdrawals, or player-to-player transfers—that collectively meet the threshold within a relevant time frame.

Prevailer B.V. actively monitors all financial activity on a continuous basis. Transaction data is aggregated daily to ensure that the cumulative behavior of each player is considered when assessing risk exposure and determining the need for additional due diligence.

When the threshold of NAF 4,000 is met, the company conducts a comprehensive customer risk assessment. This includes reviewing all previously collected information, completing any outstanding CDD obligations, and updating the customer's risk classification as needed.

Early Execution of CDD Procedures

As a proactive measure, Prevailer B.V. aims to complete CDD procedures at the earliest opportunity—preferably during account registration—regardless of whether a financial threshold has been reached. By verifying customer identities prior to their participation in financial transactions, the company reduces the likelihood of criminal actors exploiting the platform before thorough due diligence has been conducted.

Temporary Restrictions for Incomplete CDD

In circumstances where a customer reaches the NAF 4,000 threshold before completing full CDD verification, Prevailer B.V. applies specific transactional restrictions to preserve regulatory compliance:

- If the threshold is met due to a deposit, the customer is prevented from making further deposits or withdrawals. However, they may continue using existing funds for gameplay activities.
- If the threshold is reached due to a withdrawal request, the customer's account is temporarily frozen, and all gaming activity is suspended until the verification process has been finalized.

Addressing CDD Non-Compliance

If a customer fails to submit the required CDD documentation within 30 days of reaching the NAF 4,000 threshold, Prevailer B.V. initiates corrective action. The business relationship is terminated, and depending on the circumstances, the company takes the following steps:

- If the situation gives rise to a reasonable suspicion of ML or TF, a Suspicious Transaction Report (STR) is submitted to the Financial Intelligence Unit (FIU).
- In the absence of such suspicion, the remaining funds are returned to the original deposit source (e.g., the customer's verified bank account or digital wallet).
- If there are lingering concerns about possible financial crime, the company evaluates whether the funds should be frozen in accordance with its internal escalation procedures and regulatory requirements.

Preventing Tipping-Off

Prevailer B.V. is mindful of the risks associated with tipping off a customer during account restriction or closure. In such cases, the company ensures that all actions are carried out discreetly and in accordance with legal obligations. Staff are guided by internal procedures designed to avoid breaching anti-tipping-off provisions while maintaining full regulatory compliance.

By ensuring that CDD measures are implemented swiftly and in alignment with financial activity thresholds, Prevailer B.V. strengthens its defenses against financial crime, upholds transparency, and safeguards the integrity of its gaming platform across all operational channels.

Continuous Surveillance of Existing Customers

Prevailer B.V. applies Customer Due Diligence (CDD) not only at the onboarding stage but also throughout the duration of the customer relationship. The company is committed to maintaining a high standard of compliance by performing ongoing monitoring and routine reassessments, ensuring that all client activity remains consistent with prevailing Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulations.

Ongoing Review and Risk-Based Monitoring

Customer relationships are subject to continuous due diligence measures. This includes the regular monitoring of transactions and the reassessment of customer risk profiles in light of new behaviors or patterns. Where necessary, the company re-evaluates previously collected data to ensure it remains accurate, complete, and relevant. Any deviation from expected conduct prompts further review and, where applicable, the application of enhanced scrutiny.

For customers who were previously onboarded with limited or incomplete CDD, Prevailer B.V. initiates retrospective due diligence procedures. These are prioritized based on risk, with high-risk customers undergoing immediate verification. Periodic updates are also conducted in accordance with both internal policies and regulatory guidance to ensure that CDD measures remain aligned with risk exposure and evolving compliance standards.

Reapplication of CDD Based on Risk Triggers

Prevailer B.V. applies full CDD measures to existing customers under specific conditions that indicate increased risk or regulatory necessity. These conditions include, but are not limited to:

- A material change in the customer's behavior or risk profile, such as sudden high-value transactions, relocation to a higher-risk jurisdiction, or being identified as a Politically Exposed Person (PEP).
- Legislative or regulatory amendments that require updated or additional customer verification.
- The customer engaging in one or more transactions totaling NAF 4,000 or more, which automatically triggers full identity verification and documentation review under the company's CDD policy.

Remediating Gaps in Historical CDD

In instances where customers were previously allowed to transact without complete CDD—such as during legacy onboarding procedures or prior to the implementation of current regulatory standards—Prevailer B.V. takes corrective action. High-risk customers are prioritized for immediate verification, while others are subject to a scheduled review based on the level of risk they present.

CDD is applied using a proportional and risk-sensitive approach, ensuring that resources are allocated where they are most needed and that lower-risk clients are still monitored effectively.

Verification processes may include updated identity checks, refreshed PEP and sanctions screenings, and a reassessment of the customer's source of funds and wealth.

By extending due diligence practices beyond initial onboarding and embedding them into the ongoing management of customer relationships, Prevailer B.V. strengthens its regulatory compliance, reduces its exposure to financial crime, and upholds the integrity of its platform across all customer segments.

Termination of Business Relationships

Prevailer B.V. maintains the right to terminate business relationships with customers who fail to comply with Customer Due Diligence (CDD) requirements or who present heightened financial crime risks. This measure ensures the company's adherence to Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulations while preserving the security and integrity of its operations.

Business relationships are subject to termination when a customer engages in suspicious or unexplained financial activities, fails to submit required CDD documentation within the prescribed timeframe, or is determined to pose a significant risk of involvement in money laundering or terrorist financing. The decision to terminate a relationship is subject to formal internal review and must be approved by senior management.

Prior to termination, a final review of the customer's account activity is conducted to identify any outstanding irregularities. If any transaction raises suspicion of ML, TF, or PF, Prevailer B.V. submits a Suspicious Transaction Report (STR) to the Financial Intelligence Unit (FIU) without delay. All records associated with the terminated relationship are retained securely for a minimum of five years in accordance with regulatory requirements. This approach reinforces the company's commitment to proactive risk management and ensures regulatory compliance through the entire customer lifecycle.

Third-Party Reliance for Customer Due Diligence

Prevailer B.V. may, under controlled circumstances, rely on qualified third parties to carry out specific components of the Customer Due Diligence (CDD) process. Such reliance is implemented strictly within the boundaries of applicable AML/CTF/CPF laws and does not absolve the company of its legal responsibility to ensure full compliance. Prevailer B.V. remains ultimately accountable for the accuracy, completeness, and timeliness of all CDD-related activities performed on its behalf.

When relying on a third party, the company ensures that all relevant customer identification and verification information is accessible without delay upon request. Third-party arrangements are governed by formal agreements that clearly outline data-sharing protocols, compliance obligations, and procedures for independent compliance audits. These agreements require the third party to be a regulated entity subject to robust AML/CFT supervision and to maintain an independent relationship with the customer.



Importantly, Prevailer B.V. differentiates between third-party reliance and outsourcing. In a reliance scenario, the external party performs selected CDD tasks independently, while Prevailer B.V. retains full responsibility for assessing customer risk, verifying Politically Exposed Person (PEP) status, and maintaining ongoing transaction monitoring. In an outsourcing arrangement, the third party operates under Prevailer B.V.'s direct oversight, following its internal policies and regulatory framework.

Before engaging with any third-party service provider, Prevailer B.V. conducts a comprehensive risk assessment of the provider's jurisdiction, evaluating its regulatory environment and compliance history. This is supported by intelligence from international watchdogs and enforcement bodies. Regular assessments—both quantitative and qualitative—are performed to monitor the third party's performance and ensure the effectiveness of their procedures. These reviews verify that decisions regarding business relationships and risk classification remain under the exclusive control of Prevailer B.V.

Through structured oversight and stringent regulatory controls, Prevailer B.V. ensures that any third-party involvement in CDD processes contributes to a secure, transparent, and compliant operational environment.

7. SANCTIONS

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

Monitoring and Reporting Procedures

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

Client Interaction and Transaction Verification

To maintain the integrity of our operations, all client interactions and transactions undergo meticulous checks against the latest Sanctions Lists. Automated systems facilitate real-time verifications, and our database is regularly updated to reflect current sanctions information. If a match or suspicious activity is detected, it will be reported immediately to the relevant

authorities. The company will take decisive actions, including freezing accounts or blocking transactions, to manage compliance risks effectively.

Continuous Review of Compliance Procedures

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

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

Due Diligence and Evasion Prevention

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

Staff Training and Auditing

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

8. MANAGEMENT RESPONSIBILITIES

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



Policy Review and Risk Assessment

Senior management is accountable for conducting comprehensive reviews of all relevant policies and procedures at least once each year. These reviews are guided by monthly risk assessments, enabling the identification and timely addressing of any potential vulnerabilities in internal controls and risk management practices. If any deficiencies are identified, the AML/CTF/CPF Officer can recommend necessary adjustments to the Board for approval, thus enhancing the company's risk management and compliance framework.

Employee Training Programs

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

Internal Control Framework

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

9. COMPLIANCE OFFICER

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

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

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



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

The Compliance Officer is entrusted with several essential responsibilities:

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

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

10. SUSPICIOUS ACTIVITIES

Prevailer B.V. maintains a strong commitment to detecting and reporting any activity that may be indicative of money laundering (ML) or the financing of terrorism (TF). The company recognizes that suspicious conduct may not always be overt and can present in the form of behavioral irregularities, unusual transaction patterns, or financial dealings connected to jurisdictions with elevated risk profiles. All employees are expected to remain alert and escalate any suspicions immediately to the appointed Compliance Officer.

Upon receiving a report, the Compliance Officer conducts a comprehensive evaluation of the information, applying internal guidelines and regulatory criteria to determine whether further investigative measures are required. Where appropriate, and in alignment with regulatory

obligations, the matter may be formally reported to the competent authorities, such as the Financial Intelligence Unit (FIU).

Identifying Unusual Transactions

Prevailer B.V. defines an unusual transaction as any financial activity that deviates materially from a customer's established behavior or declared financial profile. These may include large or unexpected cash movements, transactions involving unknown or unverified third parties, or financial activity lacking a clear legal or economic purpose.

The company relies on advanced transaction monitoring systems to detect such anomalies. When flagged, these transactions are forwarded to the Compliance Officer for deeper review. Staff members are trained to recognize behavioral and transactional red flags and to act promptly in escalating concerns.

The following categories of transactions are considered particularly noteworthy and may trigger further examination or reporting:

- **Previously Reported Activities:** Transactions already identified and forwarded to judicial or law enforcement agencies—such as the police or public prosecutor—for potential links to ML or TF are automatically categorized as unusual.
- **Dealings with Sanctioned Persons or Entities:** Any transaction involving a party listed under the Sanctions National Ordinance (N.G. 2014 no. 55), or other relevant sanction regimes, is flagged and treated as unusual.
- **High-Value Transactions:** Transactions equal to or exceeding NAF 5,000—regardless of the method of payment—are subject to scrutiny. This includes:
 - Cash deposits or withdrawals at or above the threshold.
 - Purchases of gaming tokens, digital credits, or chips meeting or exceeding the limit.
 - Redemptions or payouts of winnings at or above the specified amount.
- The threshold also applies to a series of transactions that cumulatively total NAF 5,000 or more within a single gaming day. Such cumulative activity is evaluated in aggregate when determining whether reporting is necessary.

In cases where there is a reasonable basis to suspect that a transaction is connected to ML, TF, or PF—whether due to the nature of the transaction, the behavior of the client, or other risk indicators—it must be treated as suspicious and subject to internal escalation procedures.

Confidentiality in Reporting

Maintaining strict confidentiality around Suspicious Activity Reports (SARs) is fundamental to preserving the effectiveness of the company's compliance regime and fulfilling its legal obligations. Employees are strictly prohibited from disclosing any details of a SAR to the person under review or to any unauthorized third party. Breaches of this confidentiality can undermine

investigations, result in regulatory violations, and constitute a tipping-off offence under applicable legislation.

Only authorized personnel—such as the Compliance Officer and designated members of the compliance team—may handle SAR-related information. All such communications must be treated with the highest level of discretion. Prevalier B.V. provides regular training to ensure staff understand the importance of maintaining confidentiality in all aspects of the reporting process.

Violations of this confidentiality policy are treated as serious compliance breaches and may lead to disciplinary action, including termination of employment. These protocols are critical to maintaining the integrity of the reporting framework and the company's ability to respond effectively to financial crime risks.

By fostering a culture of awareness, discretion, and accountability, Prevalier B.V. strengthens its ability to identify suspicious behavior, uphold its obligations under AML/CTF/CPF regulations, and support broader efforts to prevent financial crimes across the iGaming sector.

11. AUDIT PROCEDURES

Prevalier B.V. conducts independent audits to ensure compliance with updated Curaçao gaming regulations and Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) standards. These audits are conducted either by external professionals or internal teams with expertise in AML/CTF/CPF and are independent of the company's AML compliance team. Auditors must also receive approval from the Gaming Control Board to guarantee adherence to regulatory requirements.

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

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

- **Evaluation of AML/CTF/CPF Policies and Procedures:** Confirming that policies are up-to-date and compliant with legal standards.
- **Risk Management Assessment:** Analysing the effectiveness of risk assessments and mitigation strategies.
- **Transaction Monitoring Review:** Evaluating the efficiency of systems used to detect and report suspicious activities.
- **Staff Training Evaluation:** Assessing the adequacy and effectiveness of employee training programs.

- **Reporting Mechanism Audit:** Reviewing procedures for reporting suspicious transactions and compliance issues.
- **Customer File Review:** Ensuring adherence to KYC (Know Your Customer), KYB (Know Your Business), and CDD (Customer Due Diligence) protocols.

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

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

The company acknowledges that non-compliance identified through audit results or Board evaluations may lead to penalties, including fines, operational restrictions, or even the suspension or revocation of its gaming license. Therefore, Prevailor B.V. is dedicated to collaborating closely with the Gaming Control Board to implement corrective actions and maintain compliance, thereby preventing future complications.

12. RECORD KEEPING

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

The company securely maintains detailed records, including:

- Customer identification information.
- Transaction histories.
- Suspicious activity reports (SARs).
- Staff training logs.
- Audit records.

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

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

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

13. TRAINING

Prevailer B.V. implements a comprehensive training program to equip employees with the knowledge and skills necessary to prevent money laundering, terrorist financing, and proliferation financing. This training is mandatory for all employees, including senior management, compliance officers, and customer-facing staff.

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

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

The training curriculum covers essential topics, including:

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

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

Training is delivered through workshops, online courses, and practical exercises, ensuring engagement and understanding. Regular refresher courses are conducted, with additional sessions for high-risk roles. Led by qualified professionals, the program ensures staff remain updated on the latest compliance requirements.

