



BY
KREVETKA B.V.

166108

Chuchubiweg 17, Willemstad, Curacao

AML/CTF/CPF POLICY

March 18, 2025

Next Review: March 2026

APPROVED BY THE BOARD OF DIRECTORS

A handwritten signature in blue ink, consisting of a large, stylized capital 'A' followed by a cursive 'R' and a trailing flourish.

Compliance Officer: Sergey Volf / compliance@krevetka.com

1. Policy Statement	3
2. Details of the Online Gaming Landscape	3
3. Money Laundering	4
4. Terrorism Financing	6
5. Evaluation of Money Laundering (ML), Terrorist Financing (TF) & Proliferation Financing (PF) Risks	7
5.1. Core Components of the Risk-Based Approach	7
5.2. Compliance with Curaçao's New Legislation	9
5.3. Risks in Technological Developments	10
6. Customer Due Diligence	11
6.1. When CDD Measures Apply	11
6.2. Details of CDD Measures	11
6.3. Player Identification and Verification	12
6.4. Understanding the Business Relationship	12
6.5. Existing Customers CDD Measures	13
6.6. Enhanced Due Diligence (EDD)	14
6.7. Simplified Due Diligence (SDD)	14
6.8. Handling Politically Exposed Persons (PEPs)	14
6.9. CDD Timing	14
6.10. Termination of Relationships	16
7. Sanctions	18
8. Identifying and Reporting Suspicious Activity	19
9. Responsibilities of the Management	21
10. Compliance Officer	22
11. AML/CTF Audit	23
12. Training	24
13. Record Keeping	25
14. Appendices	26

1. Policy Statement

KREVETKA B.V. has established its Anti-Money-Laundering/Counter-Terrorism Financing/Counter-Proliferation Financing Policy (AML/CTF/CPF Policy) to combat money laundering and terrorist financing. This policy is designed to meet both local and international standards for AML/CTF/CPF (Anti-Money Laundering/Counter Terrorism Financing/Counter-Proliferation Financing) and to ensure compliance with relevant regulations. It offers a comprehensive framework for managing risks associated with various aspects such as customer interactions, products and services, payment methods, geographical regions, and delivery mechanisms.

The Board of Directors (BoD) at KREVETKA B.V. is responsible for the approval, implementation, and oversight of the AML/CTF/CPF Policy. This policy is reviewed on an annual basis and may be updated as needed to incorporate significant changes in AML/CTF/CPF regulations or operational procedures. In addition, urgent revisions may be proposed by a designated officer following recommendations from internal and external AML audits, considering the potential risks and impacts.

The AML/CTF/CPF Policy is aligned with the primary international objectives outlined by Curaçao's AML/CTF/CPF legislation, 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), with amendments effective as of May 16, 2024. It also complies with the Sanctions National Ordinance (SNO) and the Kingdom Sanction Act.

Furthermore, this policy integrates international regulations and guidelines, including the Financial Action Task Force (FATF) Recommendations, the European Anti-Money Laundering Directives (4th, 5th, and 6th AMLDs), and the Wolfsberg Principles.

In essence, KREVETKA B.V.'s AML/CTF/CPF Policy has been crafted to adhere to the standards set by Curaçao's AML/CTF/CPF supervisory authority, the Curaçao Gaming Control Board. All directors, officers, and employees of the company, as well as any third-party consultants engaged for audit purposes, are expected to follow and uphold the principles outlined in this policy.

2. Details of the Online Gaming Landscape

KREVETKA B.V. (166108), a legal entity based in Curaçao, owns and manages the website <https://pongbet88.com/en>. The company operates under an online gaming license from Curaçao Gaming Control Board, specifically OGL/2024/937/0857, adhering

to the licensing requirements and regional restrictions set by Curaçao's regulatory authorities. These regulations forbid their remote gaming licensees from offering services in the United States, Australia, Dutch West Indies (Aruba, Bonaire), Curaçao, France, Germany, the United Kingdom, Belize, and the Netherlands. Consequently, the company only operates in markets where online gambling is legally permitted and does not target customers in jurisdictions where it is prohibited.

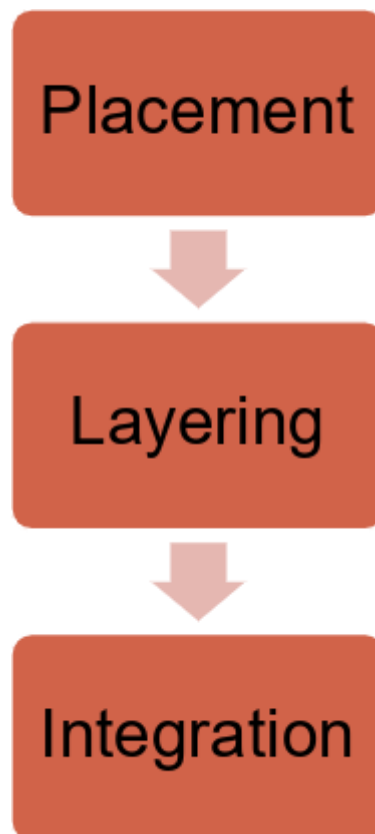
E-gaming and betting operators, including KREVETKA B.V., face various money laundering risks such as identity theft, fraud, structuring, layering, and potential collusion between employees and customers or external payment providers to circumvent internal security measures.

3. Money Laundering

Money laundering is a critical element of financially motivated crime, often spanning international borders. It plays a role in various illegal activities such as tax evasion, sanctions breaches, fraud, corruption, illegal arms dealing, drug trafficking, extortion, and kidnapping. The primary goal of money laundering is to obscure the illegal origins of the proceeds from these crimes by disguising their identity, source, and destination.

Key Stages of Money Laundering:

1. **Placement:** This is the initial phase where illicit funds are introduced into the financial system. Methods include depositing money into bank accounts, buying valuable items, or conducting other financial transactions. The objective is to begin integrating these funds into the legitimate economy.
2. **Layering:** In this stage, the money undergoes a series of intricate transactions to obscure its origin. This may involve transferring funds between multiple accounts, converting them into different currencies, or investing in various financial products. The aim is to create a complex web of transactions that hides the audit trail and makes it difficult to trace the funds back to their original source.
3. **Integration:** The final stage involves reintroducing the laundered money into the legitimate economy. This can be done through purchasing luxury goods, investing in businesses that handle a lot of cash, or engaging in other legal financial activities. By this point, the money appears legitimate and is much harder to trace back to its illicit origins.



Money laundering can occur at various stages, and online gambling platforms may be exploited as part of this process. This highlights the need for the company to avoid offering anonymous services or facilitating suspicious transactions.

Relation to Terrorist Financing

Terrorist financing refers to the funds used to support terrorist activities. These funds can come from legitimate sources but are often funneled through financial systems in a manner similar to money laundering. For instance, prepaid cards are commonly used to purchase materials for terrorist attacks. Hence, the staff is trained on the latest developments in this area.

Risk Management and Compliance

To mitigate money laundering risks, the company focuses on detecting and addressing potential threats. Key strategies include:

- **Verification Fraud and Identity Theft:** Conducting thorough customer due diligence, including verifying documentation, age, and location.
- **Operation of Multiple Accounts and High Transaction Volumes:** Monitoring for unusual activity involving multiple accounts or large transaction volumes.
- **Illicit Fund Deposits:** Identifying and addressing funds deposited from illicit activities or using the platform as a holding space for such funds.
- **Player-to-Player Transfers:** Monitoring for the misuse of the platform for transferring funds between individuals or cashing out.

This list is not exhaustive, as additional risks may arise. The company regularly conducts risk assessments tailored to specific concerns and provides ongoing training to employees to enhance its internal anti-money laundering (AML) compliance programs.

4. Terrorism Financing

Terrorist financing involves the provision of funds to support terrorist activities, utilizing both legal and illegal sources. These funds are essential for executing a range of operations, from minor incidents to major attacks.

The sources of funds can be broadly categorized into legal and illegal avenues. Legal sources include legitimate businesses, donations, and other lawful financial activities, where terrorists might exploit charitable donations and business transactions to channel money. In contrast, illegal sources involve criminal activities such as drug trafficking, fraud, smuggling, and extortion, as well as money laundering practices to obscure the origins of the funds.

Funds can be transferred through various methods. Formal channels include traditional banking systems and financial institutions, where sophisticated techniques like layering and structuring are employed to avoid detection. Informal channels, such as hawala systems, operate outside official financial frameworks, making them harder to track.

Indicators of terrorist financing often include unusual transaction patterns, such as those deviating from normal business or personal behavior. This can involve large or frequent transfers to or from high-risk areas or transactions linked to known terrorist affiliates. Additionally, suspicious activities might be evident in high-risk sectors, large cash transactions, or financial actions that seem designed to conceal terrorist operations.

To combat terrorist financing, regulatory and compliance measures are crucial. The company's Anti-Money Laundering (AML) policies are designed to detect and prevent such activities through customer due diligence (CDD), transaction monitoring, and reporting suspicious activities. Sanctions lists the company adheres to include but are not limited to such lists as the Sanctions National Ordinance (SNO, N.G. 2014, no. 55); Kingdom Sanction Act (N.G. 2016, no. 54); GCB announcements, Office of Foreign Assets Control (OFAC) and the United Nations Security Council, EU Sanctions, US List of Foreign Terrorist Organizations, OFAC, etc. The lists maintained by organizations mentioned above are used by the casino to ensure transactions do not inadvertently support terrorism.

The Financial Action Task Force (FATF) provides international guidelines to address money laundering and terrorist financing, emphasizing robust policies for identifying and reporting suspicious transactions. The OFAC enforces U.S. economic and trade

sanctions and manages the Specially Designated Nationals (SDN) list, which includes individuals and entities involved in terrorism. The European Union (EU) enforces regulations to prevent the misuse of the financial system for terrorist purposes, and member states must implement effective AML measures and adhere to international sanctions. The United Nations (UN) also plays a role by imposing sanctions and maintaining lists of those linked to terrorism, contributing to global efforts to disrupt terrorist financing and limit resources available to terrorist groups.

5. Evaluation of Money Laundering (ML), Terrorist Financing (TF) & Proliferation Financing (PF) Risks

The company employs a risk-based approach (RBA), which is pivotal for implementing effective Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) strategies. This approach ensures that resources are allocated to mitigate the most significant risks. In light of the new Curaçao gaming regulations, adopting a comprehensive RBA is essential for compliance and maintaining the sector's integrity.

The new Law on Offshore Games (LOK), replaces the National Ordinance on Offshore Games of Hazard (NOOGH). This new legislation imposes stricter AML/CTF/CPF requirements on the company as a gaming operator, necessitating a thorough RBA to effectively manage risks associated with money laundering and terrorist financing.

5.1. Core Components of the Risk-Based Approach

A central aspect of the company's risk-based approach is its comprehensive risk assessment. This process involves a detailed evaluation of risks related to customers, products, services, and geographic locations. The company regularly performs these assessments to identify and address potential vulnerabilities.

Customer Risk Profile

KREVETKA B.V. adopts a risk-based approach to compliance, placing strong emphasis on evaluating the potential exposure to money laundering (ML) and terrorist financing (TF) arising from its clientele. Each customer's profile—including their transaction behavior, sources of income, and financial background—is carefully assessed to identify any vulnerabilities that could pose a compliance risk.

Certain customer profiles inherently present higher risks. For example, individuals with multiple or opaque income sources may complicate the process of verifying the legitimacy of their funds. Similarly, clients who demonstrate unpredictable financial behavior or sudden shifts in spending patterns may raise red flags. Politically Exposed Persons (PEPs) are subject to enhanced scrutiny due to the increased corruption risks associated with their public functions and access to government-linked assets.

Additional indicators of higher-risk behavior include customers whose spending habits are inconsistent with their reported income, or those who operate multiple player accounts, potentially to obscure financial activity or bypass monitoring. To address such risks, KREVETKA B.V. sets transactional benchmarks aligned with normative customer behavior, enabling more efficient detection of anomalies.

By contrast, customers with a single, documented income stream and a stable financial history are generally regarded as low-risk. Individuals falling outside of this profile—those with complex financial arrangements or irregular transaction behavior—are flagged for closer monitoring and may be subject to Enhanced Due Diligence (EDD) protocols.

Product, Service, and Transaction Risks

Not all gaming services or financial products carry the same level of risk. Some are more susceptible to abuse by criminal elements aiming to disguise or launder illicit proceeds. KREVETKA B.V. remains alert to the misuse of gaming platforms as a vehicle for financial crime.

Funds obtained through illegal activity—including fraud, trafficking, or theft—are often laundered through gambling ecosystems to mask their origin. Particular concern arises with the use of anonymous or semi-anonymous instruments such as prepaid cards, digital currencies, and gaming tokens, which present substantial traceability challenges.

Other concerning behaviors include the use of gaming accounts solely for storing or moving funds, as well as peer-to-peer transfers between players, which can be manipulated to conceal illegal financial flows. Additionally, the use of third-party financial tools—such as cards or accounts registered to individuals other than the account holder—adds further complexity to the audit trail.

Further risks emerge from ancillary financial services tied to the gaming environment, such as internal currency exchanges, credit services, and cross-platform functionalities, all of which are potential vectors for abuse. In response, KREVETKA B.V. employs robust monitoring tools, initiates EDD when warranted, and ensures full alignment with international anti-money laundering, counter-terrorist financing, and counter-proliferation financing (AML/CTF/CPF) standards.

Geographic Risk Assessment

The geographical location of a customer and the origin of their funds are critical risk indicators. Jurisdictions known for inadequate AML/CTF governance, high corruption levels, or active sanctions programs are viewed as carrying elevated exposure to ML, TF, and CPF threats. Countries linked to terrorism or weapons proliferation are scrutinized with particular caution.

To evaluate these risks, KREVETKA B.V. relies on authoritative international and regulatory sources, including but not limited to:

- FATF (Financial Action Task Force) watchlists identifying high-risk or monitored jurisdictions
- Public advisories from the Caribbean Financial Action Task Force (CFATF)
- The U.S. Department of State's INCSR (International Narcotics Control Strategy Reports)
- The European Commission's list of high-risk third countries with strategic AML/CFT deficiencies
- OFAC (Office of Foreign Assets Control) sanctions lists
- Transparency International's Corruption Perceptions Index (CPI)

KREVETKA B.V. maintains a dynamic geographic risk classification system to distinguish between low-risk and high-risk jurisdictions. Clients associated with high-risk locations are subject to Enhanced Due Diligence, and transactions involving sanctioned countries are either closely restricted or outright prohibited. This classification framework is continuously reviewed and updated to reflect shifts in international risk assessments, ensuring a secure and compliant operating environment.

Channel Risk and Preventative Measures

The avenues through which customers engage with KREVETKA B.V.—particularly those involving remote access or limited identity verification—can increase the risk of illicit financial activity. Channels that allow for user anonymity or indirect financial transactions require careful oversight.

To mitigate these risks, KREVETKA B.V. applies stringent identification protocols and verification checks, especially when handling anonymous or semi-anonymous engagement tools. The Company employs advanced technologies such as biometric ID systems and robust digital KYC (Know Your Customer) processes to verify client identities and validate the legitimacy of financial activity.

Through vigilant oversight, secure authentication mechanisms, and the integration of risk-based controls across all customer touchpoints, KREVETKA B.V. reinforces its commitment to international AML/CTF best practices and ensures a transparent, compliant, and resilient operational environment.

5.2. Compliance with Curaçao's New Legislation

In accordance with the LOK framework, the company demonstrates its compliance by developing and implementing AML/CTF/CPF programs that incorporate the RBA and are tailored to its size, nature, and complexity. Regular training is provided to employees to ensure they understand their AML/CTF/CPF obligations, focusing on the RBA and risk management. Independent audits are conducted to assess the effectiveness of the AML/CTF/CPF program and the implementation of the RBA.

5.3. Risks in Technological Developments

KREVETKA B.V. is committed to ensuring that technological innovation within the iGaming sector is not exploited for illicit purposes such as money laundering (ML) or terrorist financing (TF). As digital transformation continues to redefine operational and user experiences, the company implements robust preventative controls and adopts a forward-thinking risk management strategy. This ensures all new business activities, platform developments, and service upgrades are thoroughly vetted for compliance with regulatory standards.

Identifying and Assessing Technology-Related Risks

To proactively manage the risks associated with evolving technologies, KREVETKA B.V. conducts detailed evaluations in the following instances:

- Introduction of new gaming features or platform functionalities
- Operational improvements focused on efficiency or user experience
- Implementation of advanced payment solutions or alternative access tools
- Integration of cutting-edge technologies, such as blockchain, artificial intelligence, or enhanced cybersecurity infrastructure

Before deploying any new system, product, or tool, KREVETKA B.V. performs a rigorous risk assessment to uncover any weaknesses that may be exploited for financial crime. These reviews focus on identifying vulnerabilities and mapping them against applicable AML/CTF frameworks—both local and international. All assessments are documented to create a traceable and auditable record of risk analysis.

Applying Targeted Risk Mitigation Measures

Once potential risks are identified, KREVETKA B.V. acts promptly to implement tailored mitigation strategies. These may include:

- Reinforced Security Infrastructure
Introduction of strong identity verification processes, including multi-factor authentication (MFA), biometric verification, encrypted communications, and AI-based fraud detection systems to protect digital assets and user data.
- Enhanced Monitoring Systems
Upgrading of transaction monitoring technologies to identify suspicious behavior patterns in real time. Automated tools are used to flag activities that deviate from expected financial behavior or suggest ML/TF intent.

- **Dynamic Policy Updates**

Adaptation of the company's AML/CTF framework to reflect emerging technological threats. KREVETKA B.V. ensures that its policies evolve in parallel with advancements in financial crime techniques and cyber-enabled threats.

Through continuous evaluation and enhancement of its technological safeguards, KREVETKA B.V. reinforces its commitment to maintaining a secure, transparent, and fully compliant operational landscape. This proactive approach not only mitigates risks but also ensures that innovation is implemented responsibly—without compromising the company's regulatory obligations or exposing its financial ecosystem to criminal exploitation.

6. Customer Due Diligence

The company adheres to regulations requiring casinos to avoid anonymous or fake accounts. The company verifies players' identities and understands their business relationships as it is an essential process for casinos to combat money laundering, terrorism financing, and proliferation. A robust Customer Due Diligence (CDD) program is vital for assessing risks and ensuring compliance with behavioral expectations. Any suspicious activities are reported to the Financial Intelligence Unit (FIU) and, if necessary, to the Public Prosecutor's Office.

6.1. When CDD Measures Apply

The company implements CDD measures under the following circumstances:

- Transactions of NAF 4,000 or more.
- Occasional transactions exceeding NAF 4,000.
- Suspicion of money laundering or terrorism financing.
- Uncertainties regarding previously obtained customer identification data.
- Transactions, whether single or multiple linked transactions surpassing NAF 4,000. Even if individual transactions are below this threshold, linked transactions are subject to CDD. High-risk transactions require enhanced due diligence.

6.2. Details of CDD Measures

Identifying and Verifying Players: The company's CDD measures involve:

- Verifying player identities with legitimate, reliable, and independent documents, data, or systems.
- Identifying and confirming the ultimate beneficial owner and understanding their ownership and control structure for legal entities.
- Understanding the purpose and nature of the business relationship.

- Conducting ongoing due diligence and monitoring transactions to ensure consistency with the casino's knowledge of the player and their risk profile, including the source of funds if necessary.

Confidentiality of Reports: Staff does not disclose when a report is made to the FIU to avoid tipping off players. If suspicion of money laundering or terrorism financing arises and CDD might alert the player, the casino bypasses the process and files a report directly to the FIU.

6.3. Player Identification and Verification

Identification Process: To establish a player's identity, the following details are collected:

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

In lower-risk scenarios, only basic details are needed. For higher-risk situations, more comprehensive information is collected to mitigate risks of money laundering and terrorism financing.

Risk Assessment: Initial risk ratings are assigned based on collected information and revised as more data is available. This helps determine the appropriate level of CDD.

Verification Process: Verification ensures that a player is who they claim to be through:

- Government-issued photo ID (e.g., passport, ID card)
- Supplementary documents (e.g., utility bill, bank statement) confirming address, no older than six months
- Verification of address through letters, email, or phone
- Biometric checks, cross-referencing database information, IP addresses, and funding methods

If the information collected is insufficient, additional steps may be taken, such as requesting a selfie with the ID or verifying the first deposit through a regulated financial institution.

6.4. Understanding the Business Relationship

The company identifies the purpose and nature of its relationships with players as part of its CDD process. While the nature of the relationship might be clear, sufficient information is gathered to detect any unusual or suspicious activities. For higher-risk clients, detailed documentation of the source of wealth and expected activity levels is collected to ensure legitimacy. For lower and medium-risk players, a declaration with

basic employment or business details suffices, while independent sources are used for higher-risk clients.

6.5. Existing Customers CDD Measures

KREVETKA B.V. applies Customer Due Diligence (CDD) not as a one-time obligation, but as a continuous process throughout the entire customer relationship lifecycle. By embedding periodic reviews and dynamic risk evaluations into its broader compliance framework, the company ensures sustained alignment with Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) requirements. This practice forms part of KREVETKA B.V.'s overarching risk-based strategy, which is designed to adapt to emerging risks and maintain the integrity of its operations.

Continuous Monitoring and Risk Reassessment

Ongoing Due Diligence

CDD procedures are actively applied to both new and existing customers. Central to this approach is the ongoing monitoring of transactions and the periodic reassessment of client risk profiles to ensure that the customer's activity remains within acceptable parameters.

Tailored Risk-Based Measures

For customers who were initially onboarded with incomplete or minimal due diligence, KREVETKA B.V. conducts retrospective reviews. This includes:

- Re-evaluating and updating records for customers identified as having elevated risk;
- Scheduling routine updates to ensure that all stored data reflects the latest regulatory requirements and customer status.

When Re-Verification is Required

KREVETKA B.V. re-applies full CDD measures in any of the following circumstances:

- A significant shift in the customer's behavior or profile, such as initiating unusually large or complex transactions, moving into a high-risk jurisdiction, or being reclassified as a Politically Exposed Person (PEP);
- Regulatory or legal updates requiring refreshed or additional customer information;
- When a pre-existing customer initiates a transaction or series of transactions that meet or exceed the company's defined threshold of NAF 4,000, thereby activating the full CDD requirement under the firm's AML policy.

Remediating Gaps in Historical Due Diligence

In cases where clients were initially onboarded without full CDD being completed—often due to historical onboarding practices—KREVETKA B.V. undertakes corrective action as follows:

- Customers classified as high-risk are given priority for immediate identity and risk reassessment;
- Full CDD is applied systematically at intervals based on the specific risk rating assigned to the customer.

By ensuring that customer profiles are consistently reviewed and verified over time, KREVETKA B.V. strengthens its AML/CTF/CPF compliance posture, mitigates exposure to financial crime, and maintains a secure and transparent environment within its gaming operations.

6.6. Enhanced Due Diligence (EDD)

For high-risk scenarios, EDD measures are applied, including:

- In-depth investigation into the player's background.
- Verification of source of funds and wealth.
- Close examination of transaction patterns.
- Regular updates of identification information.

EDD also applies to politically exposed persons (PEPs), requiring thorough risk assessments and ongoing monitoring.

6.7. Simplified Due Diligence (SDD)

For low-risk scenarios, Simplified Due Diligence (SDD) measures apply, which include collecting basic customer information and conducting less frequent reviews. SDD allows for a streamlined process, though enhanced measures will be implemented if suspicious activities arise or the player's risk profile changes.

6.8. Handling Politically Exposed Persons (PEPs)

The company's AML/CTF/CPF policy requires heightened scrutiny for PEPs, their family members, and close associates. Enhanced Due Diligence (EDD) measures include obtaining senior management approval, understanding the source of funds and wealth, and conducting rigorous ongoing monitoring.

6.9. CDD Timing

KREVETKA B.V. enforces Customer Due Diligence (CDD) measures swiftly and in alignment with established obligations under Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) regulations. These measures are designed to ensure that all customer identities are accurately established and verified before significant financial interaction occurs.

Trigger Points for CDD Based on Transaction Activity

Upon the creation of a player account, KREVETKA B.V. collects and verifies key identity details from each user, including:

- Full legal name
- Residential address
- Date of birth
- Politically Exposed Person (PEP) status
- Sanctions screening

As part of the company's risk-based compliance framework, identity verification is initiated prior to processing any financial transaction that meets or exceeds a threshold of NAF 4,000. This threshold is applied in the following scenarios:

- A single transaction equal to or above NAF 4,000
- A combination of transactions (such as multiple deposits, withdrawals, or internal transfers) that cumulatively reach this amount

Daily transaction data is monitored and aggregated per customer, enabling the company to identify when thresholds are met and respond in real time. Once the NAF 4,000 mark is reached, a full risk evaluation of the customer is conducted, and any remaining CDD steps are completed without delay.

Proactive CDD Measures at Onboarding

KREVETKA B.V. emphasizes early completion of CDD. Identity checks are conducted at the point of registration, regardless of financial thresholds. This preemptive strategy is intended to prevent the entry of illicit funds into the system by ensuring that no user is granted full platform access without having first undergone due diligence.

Operational Limits for Incomplete CDD

- In situations where a player reaches the NAF 4,000 threshold prior to completing CDD, specific limitations are imposed:
- If triggered by a deposit: Further deposits and withdrawals are restricted; however, the customer may continue to participate in gaming using their current account balance.

If triggered by a withdrawal request: The player's account is temporarily frozen, and all gameplay is suspended until full verification is completed.

These safeguards help preserve the integrity of the platform and prevent unauthorized movement of funds during the verification window.

Consequences of CDD Non-Compliance

If a customer fails to submit the required documentation within 30 days after reaching the transaction threshold, the following measures are taken:

- The business relationship is terminated;
- If there are grounds for suspicion of ML or TF, a Suspicious Transaction Report (STR) is filed with the Financial Intelligence Unit (FIU);
- In the absence of suspicion, any remaining funds are returned to the source of deposit (e.g., the original bank account or digital wallet);
- Where suspicion persists, internal policies determine whether funds should be frozen pending further investigation, ensuring compliance with applicable law.

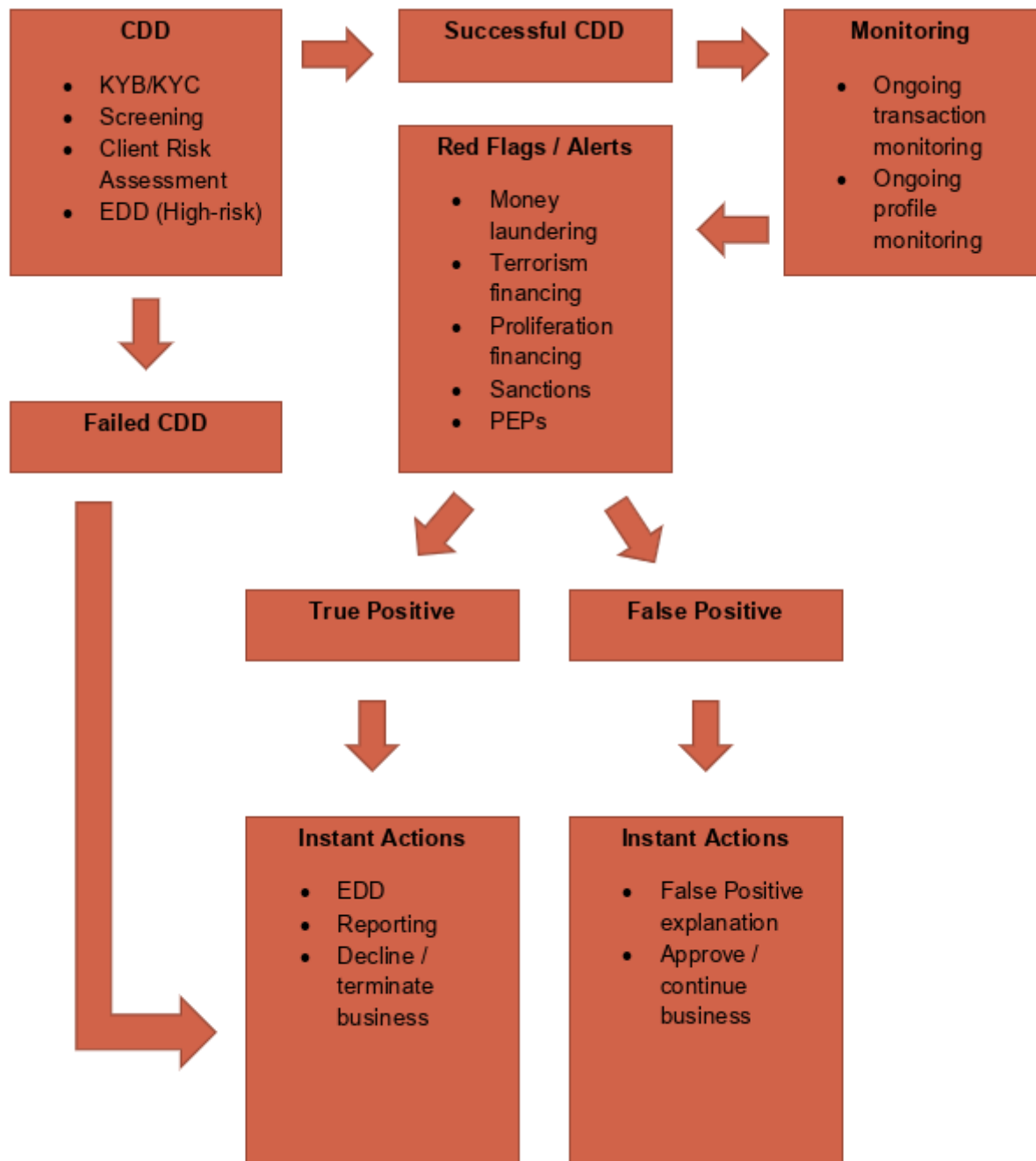
Preventing Tipping-Off

KREVETKA B.V. is conscious of the legal prohibition against tipping-off under AML/CTF legislation. Measures such as account restrictions or termination are assessed carefully to avoid alerting customers prematurely. Internal procedures guide staff on how to manage communication and actions in a way that respects confidentiality and regulatory obligations.

By integrating timely, risk-based, and proactive CDD practices into its operations, KREVETKA B.V. ensures comprehensive adherence to AML/CTF/CPF standards, minimizes exposure to financial crime, and fosters a secure and transparent environment for both digital and physical gaming channels.

6.10. Termination of Relationships

If a player engages in suspicious activities or fails to provide adequate information, the casino reserves the right to terminate the relationship. The decision must be documented and approved by senior management. Upon termination, all activities are reviewed, and any suspicious transactions are reported to the FIU. Records of the terminated relationship are securely stored for at least five years.



7. Sanctions

Our AML/CTF/CPF policy mandates rigorous compliance with both international sanctions and regulatory standards. To ensure we meet these obligations, we implement comprehensive procedures focused on adhering to all sanctions imposed by national and international authorities. This process involves conducting thorough due diligence on every client and transaction to prevent any interactions with sanctioned individuals, entities, or regions.

Monitoring and reporting are critical components of the company's AML/CTF/CPF policy. The company continuously observes all transactions for any suspicious activities that could breach sanctions. Any anomalies detected are reported immediately to the relevant authorities. Furthermore, the company's commitment to compliance is reinforced through ongoing staff training, which ensures that all personnel are up-to-date with current sanctions regulations. This approach safeguards our operations and helps mitigate potential risks.

In addition, the company is dedicated to ensuring that all client interactions and transactions are meticulously checked against the most recent Sanctions Lists. Automated systems perform real-time verifications, and our database is regularly updated to reflect the latest sanctions information. When a match or suspicious activity is identified, it is promptly reported to the appropriate authorities. The company takes decisive action, such as freezing accounts or blocking transactions, to address and manage compliance risks.

Our sanctions compliance procedures are subject to frequent reviews and updates to align with evolving legislation. This includes monitoring lists such as:

- 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.

Our due diligence efforts are designed to uncover indirect or covert attempts to engage with sanctioned parties or jurisdictions. Any discovered evasion tactics are swiftly reported to the relevant authorities, and corrective actions, including transaction suspensions and account reviews, are promptly implemented. Regular audits and ongoing staff training further ensure that the company remains vigilant and compliant with the latest legislative requirements and best practices for preventing sanctions evasion.

8. Identifying and Reporting Suspicious Activity

KREVETKA B.V. maintains a proactive approach to detecting and reporting behaviors that may indicate money laundering or terrorist financing. These behaviors could include irregular customer conduct, large or frequent transactions that fall outside expected norms, or associations with jurisdictions considered high-risk. All staff members are expected to remain alert to these red flags and must promptly communicate any concerns to the appointed Compliance Officer. Upon receiving such reports, the Compliance Officer conducts a thorough evaluation to determine whether the activity warrants escalation or notification to the relevant regulatory bodies.

Indicators of Unusual Transactions

Unusual transactions are those that deviate significantly from a customer's established financial behavior or profile. These might include unexpectedly high-value transactions, activity involving unknown third parties, or transfers that appear to serve no clear legal or economic function. KREVETKA B.V. leverages transaction monitoring systems to flag such anomalies, which are then forwarded to the Compliance Officer for detailed review.

Under the regulatory standards governing KREVETKA B.V., the following categories of transactions—whether completed or attempted—are considered potentially unusual and may require further investigation or formal reporting:

- **Previously Reported Suspicious Activity:**
Any transaction that has already been submitted to law enforcement, such as the Police or the Department of Justice, for its suspected connection to money laundering (ML) or terrorist financing (TF) is classified as unusual by default.
- **Transactions Involving Sanctioned Parties:**
Any transaction carried out by or on behalf of individuals, legal entities, or organizations listed under the *Sanctions National Ordinance (N.G. 2014 no. 55)*, or appearing on other official sanction lists, is deemed unusual.
- **Transactions at or Above NAF 5,000:**
Regardless of the method—cash, electronic, check, or other payment formats—any transaction reaching this threshold is subject to enhanced scrutiny. Examples include:
 - Deposits or withdrawals of NAF 5,000 or more
 - Purchase of chips or credits in the same amount, including physical or digital equivalents
 - Payouts or redemptions that meet or exceed the threshold

- This applies not only to single transactions but also to series or combinations of smaller transactions that together total NAF 5,000 within a single day.
- Transactions Suggesting ML or TF Activity:
If there are reasonable grounds to believe that a transaction may be linked to financial crime—based on contextual indicators or suspicious patterns—it must be treated as unusual and escalated accordingly.

Evaluation and Filing Procedures

When a report of an unusual transaction is received, the Compliance Officer reviews the information using internal risk parameters and regulatory standards. If the activity is deemed suspicious, a formal report is filed with the Financial Intelligence Unit (FIU) in compliance with Curaçao's AML framework. This decision is made after a comprehensive analysis to ensure it meets the legal threshold for suspicious activity.

Safeguarding the Confidentiality of the Reporting Process

To protect the integrity of the reporting mechanism and uphold legal obligations, KREVETKA B.V. enforces a strict confidentiality policy around Suspicious Activity Reports (SARs). Information related to such reports must never be disclosed to the individual involved or to unauthorized third parties. Maintaining this confidentiality is essential to avoid jeopardizing potential investigations or enforcement actions.

Employees are instructed to treat all communications regarding SARs with extreme discretion and are only permitted to discuss them with the Compliance Officer or other duly authorized personnel. Breaches of this confidentiality protocol are considered serious violations of the company's AML framework and may result in disciplinary consequences.

By maintaining this structured and secure process, KREVETKA B.V. ensures that the detection and reporting of suspicious activity are conducted in a lawful, confidential, and effective manner—thereby contributing to the broader fight against financial crime.

Confidentiality in Reporting Suspicious Activity

To maintain the integrity of its reporting framework and meet legal and regulatory obligations, KREVETKA B.V. enforces a strict confidentiality policy concerning Suspicious Activity Reports (SARs). Under no circumstances are employees permitted to disclose information related to a SAR to the person or entity involved, or to any unauthorized individuals. This safeguard is essential to avoid tipping off potential subjects, disrupting ongoing investigations, or compromising legal proceedings.

All matters involving the reporting of suspicious activity are handled with the highest level of discretion. Communications of this nature are restricted to the Compliance Officer and other authorized personnel only. Employees receive specific training that underscores the importance of confidentiality as a foundational element of the

company's Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) program.

Any breach of this confidentiality protocol is regarded as a serious violation of company policy and may result in disciplinary consequences, including possible termination of employment. These controls are in place to ensure that the reporting mechanism remains secure, effective, and fully compliant with applicable legislation.

Through a culture of discretion and accountability, KREVETKA B.V. demonstrates its commitment to safeguarding the integrity of its operations while aligning with Curaçao's regulatory expectations and global AML/CTF best practices.

9. Responsibilities of the Management

The role of senior management in the company is pivotal for evaluating and managing the risks associated with AML/CTF/CPF. To ensure proper oversight, the Board of Directors requires the appointed AML/CTF/CPF Officer to provide regular updates on any major changes or issues in the control environment. This officer is also tasked with delivering an annual report that assesses the effectiveness of the Company's measures and controls designed to counteract risks related to money laundering, terrorist financing, and proliferation financing.

Senior management is responsible for conducting thorough reviews of all relevant policies and procedures at least once a year. These reviews are informed by monthly risk assessments, which help in identifying and addressing any potential weaknesses in internal controls and risk management practices in a timely manner. If deficiencies are found, the AML/CTF/CPF Officer can propose necessary adjustments to the Board for approval, thereby strengthening the Company's risk management and compliance efforts.

Consistent with global best practices, senior management is also tasked with overseeing the development and implementation of comprehensive employee training programs. These programs aim to boost awareness and knowledge of AML/CTF/CPF risks among employees, particularly those in critical roles, to ensure they can effectively recognize and respond to suspicious activities.

Additionally, senior management ensures that the Company's internal control framework is solid and encompasses adequate segregation of duties, clear authorization processes, ongoing monitoring, and thorough documentation. To maintain regulatory compliance and enhance the AML/CTF/CPF program's effectiveness, regular independent audits and assessments are conducted to provide an objective evaluation and identify areas for improvement.

10. Compliance Officer

Our company designates a qualified individual to serve as the Compliance Officer. This appointment is a pivotal aspect of our Anti-Money Laundering (AML) strategy and is made by senior management to ensure the role's autonomy and authority. The appointed Compliance Officer has substantial expertise in AML compliance and holds a senior position to effectively supervise the implementation of AML policies and procedures. The role is formalized through an appointment letter that details their responsibilities and the organizational reporting structure.

The Compliance Officer undertakes several critical functions to ensure the effectiveness of our AML program. Their primary duties include:

- **Policy Implementation:** Overseeing the execution of AML policies and procedures and ensuring they align with current regulations.
- **Central Point of Contact:** Acting as the main contact for all AML-related concerns.
- **Policy Review:** Regularly reviewing and updating AML policies to reflect evolving regulatory standards and emerging risks.
- **Training Oversight:** Managing the AML training program, ensuring employees are well-informed about AML requirements and their roles in maintaining compliance.

The Compliance Officer is entrusted with several core responsibilities:

1. **Transaction Monitoring and Reporting:** Continuously analyzing transactions and client activities to detect suspicious behavior. They are responsible for filing Suspicious Activity Reports (SARs) with the Financial Intelligence Unit (FIU) when necessary and maintaining accurate records of these reports.
2. **Policy Development and Updates:** Crafting and revising AML policies and procedures to comply with the latest Curaçao gaming regulations and international best practices. This involves adjusting the AML framework to mitigate new risks and regulatory changes.
3. **Employee Training and Awareness:** Ensuring that all staff receive thorough AML training and understand their responsibilities in detecting and reporting suspicious activities. The Compliance Officer must regularly update training materials to stay current with legislative or policy changes.
4. **Regulatory Liaison:** Serving 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.
5. **Compliance Audits:** Conducting regular reviews and audits of the AML program to assess its effectiveness and adherence to legal requirements. The Compliance Officer must address any identified issues and implement corrective measures as needed.

6. Record-Keeping: Keeping 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 accessible for regulatory review.

By executing these functions and responsibilities, the Compliance Officer plays a crucial role in protecting the organization from money laundering and terrorist financing risks, ensuring rigorous compliance with Curaçao's AML regulations.

11. Audit

To align with the new gaming regulations in Curacao, the company undergoes an independent audit focused on Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF). This section provides a comprehensive guide to the audit process, detailing the role of the independent auditor and the review conducted by the Gaming Control Board.

The primary aim of the annual AML/CTF/CPF audit is to evaluate the effectiveness and compliance of the company's AML/CTF/CPF practices. This audit helps the company meet up-to-date legal standards and best practices to mitigate risks associated with money laundering and terrorism financing. The audit encompasses a detailed examination of the AML/CTF/CPF program, including risk assessments, transaction monitoring, staff training, and reporting procedures.

The company engages an external auditor or an internal audit team with the appropriate resources and expertise in AML/CTF/CPF. This auditor is independent of the company's AML Compliance team to avoid any conflicts of interest. The auditor's credentials, experience, and industry reputation are considered by the company. The Company is aware that The Gaming Control Board must approve the chosen auditor to ensure compliance with Curacao's gaming regulations.

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

- Evaluation of AML/CTF/CPF Policies and Procedures: Ensure they are updated and compliant with legal standards.
- Risk Management Assessment: Analyze the effectiveness of risk assessments and mitigation strategies.
- Transaction Monitoring Review: Check the efficiency of systems for detecting and reporting suspicious activities.
- Staff Training Evaluation: Assess the adequacy and effectiveness of employee training programs.
- Reporting Mechanism Audit: Examine the procedures for reporting suspicious transactions and compliance issues.

- Customer File Review: Verify compliance with KYC (Know Your Customer), KYB (Know Your Business), and CDD (Customer Due Diligence) protocols.

Following the audit, the independent auditor produces a detailed report outlining their findings, recommendations, and any issues identified. This report is delivered to the company's senior management and the Gaming Control Board. The company will address the auditor's recommendations and implement corrective actions within a set timeframe. Subsequent audits may be required to ensure that corrective measures are effectively applied.

The Gaming Control Board oversees AML/CTF/CPF compliance for all licensed operators, including reviewing audit results and conducting its own evaluations, hence, the company is aware that the Board can request additional documents, perform inspections, and review the implementation of audit recommendations.

The examination process by the Board includes:

- Audit Report Review: The Board will analyze the auditor's report to assess compliance and identify any concerns.
- Onsite Inspections: The Board may visit the premises to verify audit findings and assess the effectiveness of corrective actions.
- Interviews and Documentation Analysis: The Board will interview relevant staff and review documentation to thoroughly understand the company's AML/CTF/CPF practices.

The Company is aware that if it is found to be non-compliant based on audit results or Board examinations, it may face penalties, ranging from fines and operational restrictions to suspension or revocation of its gaming license. The company will work closely with the Gaming Control Board to ensure corrective actions are taken and maintain compliance to avoid future issues.

12. Training

The company has established a robust training program focusing on AML/CTF/CPF for its employees.

The primary goal of the AML/CTF/CPF training is to arm employees with the essential knowledge and skills required to identify and prevent activities related to money laundering and terrorism financing. This training ensures that employees are well-versed in their legal obligations, capable of recognizing suspicious behavior, and familiar with the procedures for reporting such activities. An informed workforce is key to the successful application of AML/CTF/CPF policies, which in turn supports the integrity and credibility of the gaming industry.

The training is tailored to fit the specific needs of different roles within the company and is mandatory for all staff members. This includes senior management, compliance officers, customer-facing personnel, operational staff, and anyone else involved in financial transactions or interactions with customers.

New hires receive comprehensive initial training, and all employees participate in refresher courses at least once a year. For roles with heightened exposure to AML/CTF/CPF risks, additional training sessions may be scheduled more frequently.

The program encompasses a range of critical topics. Employees are educated on AML/CTF/CPF laws and regulations specific to Curacao, as well as the company's internal policies and procedures related to AML/CTF/CPF. Training also covers the roles and responsibilities of employees in maintaining compliance, the process for customer identification and verification (including KYC/CDD procedures), and how to identify and report suspicious activities. Additionally, employees learn about record-keeping requirements, the consequences of non-compliance, and emerging trends in money laundering and terrorism financing.

To ensure the training is effective and accessible, a mix of delivery methods is utilized. These include in-person workshops, online courses, interactive e-learning modules, and practical exercises such as case studies and role-playing scenarios. This varied approach accommodates different learning styles and reinforces key concepts.

Training sessions are led by qualified professionals with expertise in AML/CTF/CPF. This may involve internal compliance officers or external consultants who are up-to-date with the latest legal requirements and industry practices. The goal is to ensure that the training content is current, relevant, and accurately reflects the latest developments in AML/CTF/CPF compliance.

13. Record Keeping

To meet record-keeping standards, the company adheres to stringent practices for managing AML/CTF/CPF documentation. Our approach involves the detailed retention of records such as customer identification, transaction data, suspicious activity reports (SARs), training records, and audit logs for at least five years.

These records are securely protected through encryption and robust access controls, preventing unauthorized access. We conduct regular security audits to ensure that data remains intact and uncompromised.

The organization employs a systematic method for organizing records to facilitate swift retrieval. This setup allows both authorized staff and regulatory bodies to access the information efficiently. To maintain compliance, we carry out continuous internal monitoring and periodic audits.

By managing records effectively, the company not only fulfills regulatory requirements but also supports auditing processes and upholds the integrity of the gaming industry.

14. Appendices

Appendix 1 (Key Definitions)

The Curaçao Gaming Control Board (GCB): acts as the Supervisory Authority responsible for ensuring AML/CFT compliance across the entire gaming industry.

CFATF: The Caribbean Financial Action Taskforce, consisting of 24 member countries from the Caribbean Basin, Central, and South America, committed to enforcing unified measures to combat money laundering.

Compliance Officer: A high-ranking officer, independent from gaming operations, tasked with identifying and preventing money laundering and terrorist financing activities.

FATF: The Financial Action Task Force, an international organization formed in 1989, which develops and promotes policies to safeguard the global financial system from money laundering, terrorist financing, and the spread of weapons of mass destruction.

FATF Recommendations: Guidelines and policies developed by the FATF to counter money laundering, terrorist financing, and the proliferation of weapons of mass destruction.

Financial Transactions: In casinos, these include the buying or cashing in of casino chips or tokens, opening accounts, wire transfers, and currency exchanges. This term excludes transactions limited to casino chips or tokens.

FIU The Financial Intelligence Unit Curaçao, referred to in part 2 of the NORUT.

Kingdom Sanctions Act: The National Ordinance, also known as the "Rijkssanctiewet," published under N.G. 2016 no. 54.

NOIS: The National Ordinance on Identification of Clients when providing Services (Landsverordening Identificatie bij dienstverlening, N.G. 2017, no. 92).

NORUT: The National Ordinance on Reporting of Unusual Transactions (Landsverordening Melding Ongebruikelijke Transacties, N.G. 2017, no. 99).

Other online games: Includes sports betting, esports betting, fantasy sports, lottery and bingo, skill-based games, and virtual sports.

Politically Exposed Persons (PEPs): Foreign PEPs are individuals who currently hold or have held significant public roles in a foreign country, along with their immediate family members and close associates. Examples include heads of state or government, senior politicians, top-level government, judicial or military officials, senior executives of state-owned enterprises, and key political party officials. Domestic PEPs are individuals who currently hold or have held significant public roles within their own country, such as heads of state or government, senior politicians, high-ranking government, judicial or military officials, senior executives of state-owned enterprises, and key political party officials. Additionally, those who have significant roles in international organizations, such as directors, deputy directors, and board members, are also considered PEPs.

Sanctions National Ordinance: Also known as the "Sanctielandsverordening," published under N.G. 2014 no. 55.

Source of Funds: Refers to the origin of the money used in a specific transaction by a player, including personal savings, pension payouts, property sales, stock sales and dividends, gambling winnings, gifts, and compensation from legal judgments.

Source of Wealth: Refers to the total accumulation of money a person has acquired over their lifetime, including income, inheritances, investments, and business interests.

Unusual Transaction: A transaction identified as unusual based on specific criteria, as outlined in Article 10 of the NORUT.

(Ultimate) Beneficial Ownership (UBO): Refers to the actual individual(s) who ultimately own or control a customer or the person on whose behalf a transaction is being conducted, including those who exert ultimate effective control over a legal entity.